© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 03 | 22 | April-June 2016
Paper is available at www.jrps.in | Email : info@jrps.in

SECURING IMAGE BASE OF IRIS SECURITY SYSTEM USING CRYPTOGRAPHIC TECHNIQUES

VAISHALI BHATIA , Research Scholar, Department of CSE, OM INSTITUTE OF TECHNOLOGY AND MANAGEMENT
DR. ANUJ SHARMA, Department of CSE, OM INSTITUTE OF TECHNOLOGY AND MANAGEMENT

Abstract: Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex random patterns are unique, stable, and can be seen from some distance. Databases of enrolled templates are searched by matcher engines at speeds measured in the millions of templates per second per CPU, and with remarkably low false match rates. But here issue is that stored biometric sample is stolen by hacker than they can be missing used. The objective of our research is to secure the biometric samples taken during scanning using encryption mechanism. So if hacker does steal any information then he will not be able to understand it. Biometric security is nothing if the biometric samples are not secure.

[I] IRIS RECOGNITION SYSTEMS

Several hundred millions of persons in several countries around the world have been enrolled in iris recognition systems, for convenience purposes such as passport-free automated border-crossings, and some national ID systems based on this technology are being deployed. The iris-scan process begins with a photograph. A specialized camera, typically very close to the subject, not more than three feet, uses an infrared imager to illuminate the eye and capture a very high-resolution photograph. This process takes 1 to 2 seconds. A key advantage of iris recognition, besides its speed of matching and its extreme resistance to false matches is the stability of the iris as an internal and protected, yet externally visible organ of the eye.

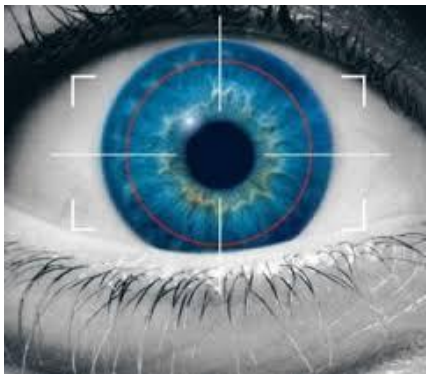


Fig:1 Human eye

[II] Iris as a powerful identifier

Iris is the focus of a relatively new means of biometric identification. The iris is called the living password because of its unique, random features. It is always with you and cannot be stolen or faked. The iris of each eye is absolutely unique. Probability that any two irises could be alike is one in 10 to 78^{th} power the entire human population of the earth is roughly 5.8 billion. So no two irises are alike in their details, even among identical twins. Even the left and right irises of a single person seem to be highly distinct. Every iris has a highly detailed and unique texture that remains stable over decades of life. Because of the texture, physiological nature and random generation of an iris artificial duplication is virtually impossible.

[II] THREATS TO BIOMETRIC SAMPLES

There are several threat to Biometric Samples

Security exploits

A security exploit is a prepared application that takes advantage of a known weakness. Common examples of security exploits are SQL injection, Cross Site Scripting and Cross Site Request Forgery which abuse security holes that may result from substandard programming practice. Other exploits would be able to be used through FTP, HTTP, PHP, SSH, Telnet and some web-pages. These are very common in website/domain hacking. Hacking Techniques

Vulnerability scanner

A vulnerability scanner is a tool used to quickly check computers on a network for known weaknesses. Hackers also commonly use port scanners. These check to see which ports on a specified computer are "open" or available to access

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 03 | 22 | April-June 2016
Paper is available at www.jrps.in | Email : info@jrps.in

the computer, and sometimes will detect what program or service is listening on that port, and its version number. (Firewalls defend computers from intruders by limiting access to ports and machines, but they can still be circumvented.)

Password cracking

Password cracking is the process of recovering passwords from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password.

Packet sniffer

A packet sniffer is an application that captures data packets, which can be used to capture passwords and other data in transit over the network.

Spoofing attack (Phishing)

A spoofing attack involves one program, system or website that successfully masquerades as another by falsifying data and is thereby treated as a trusted system by a user or another program—usually to fool programs, systems or users into revealing confidential information, such as user names and passwords. ***Rootkit***

A rootkit is a program that uses low-level, hard-to-detect methods to subvert control of an operating system from its legitimate operators. Rootkits usually obscure their installation and attempt to prevent their removal through a subversion of standard system security. They may include replacements for system binaries, making it virtually impossible for them to be detected by checking process tables.

[III]CRYPTOGRAPHY

Cryptography, which translates as "secret writing," refers to the science of concealing the meaning of data so only specified parties understand a transmission's contents. Cryptography has existed for thousands of years; for most of history, however, the users of cryptography were associated with a government or organized group and were working to conceal secret messages from enemies. These days, millions upon millions of secure, encoded transmissions happen online each day -- and cryptographic standards are used to protect banking data, health information, and much more. Without cryptography, e-commerce as we know it would be impossible. Since online security threats evolve so quickly, there are dozens of different schools of thought on how best to use encryption to enhance network security -- not just for governments, but for businesses and end users, too.

Cryptography is the science of providing security for information. It has been used historically as a means of providing secure communication between individuals, government agencies, and military forces. Today, cryptography is a cornerstone of the modern security technologies used to protect information and resources on both open and closed networks.

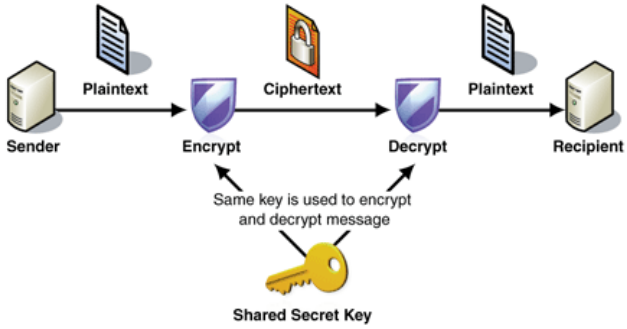


Fig 2. Cryptography

No system of cryptography, called a *cryptosystem*, can be considered absolutely unbreakable or beyond compromise. However improbable a successful attack might seem, there is always some facet of the cryptosystem that can be attacked. The history of cryptography is full of examples of cryptosystems that were once considered invincible, and yet people were able to break the security and compromise them. Because cryptographers are not omniscient, they cannot design cryptosystems that are guaranteed to have no weaknesses or that are impervious to unforeseeable methods of attack. Furthermore, cryptosystems must be implemented in the real word, so they are subject to real-world limitations and constraints. All information security systems, including cryptography-based security, have weak links that can be attacked and potentially exploited to compromise the system.

[IV]NEED OF RESEARCH

Iris-based identification and verification technology has gained acceptance in a number of different areas. Application of iris recognition technology can he limited only by imagination. The important applications are those following: ATM and iris recognition: in U.S many banks incorporated iris recognition technology into ATM for the purpose of

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 03 | 22 | April-June 2016
Paper is available at www.jrps.in | Email : info@jrps.in

controlling access to one bank accounts. After enrolling once (a 30 second process), the customer need only approach the ATM, follow the instruction to look at the camera, and be recognized within 2-4 seconds. The benefits of such a system are that the customer who chooses to use bank ATM with iris recognition will have a quicker, more secure transaction. Iris scan has implemented their devices with great success in prisons in Pennsylvania and Florida. By this any prison transfer or release is authorized through biometric identification. Such devices greatly ease logistical and staffing problems. Applications of this type are well suited to iris recognition technology. First, being fairly large, iris recognition physical security devices are easily integrated into the mountable, sturdy apparatuses needed or access control, The technology phenomenal accuracy can be relied upon to prevent unauthorized release or transfer and to identify repeat offenders re-entering prison under a different identity. Computer login: The iris as a living password.

National Border Controls: The iris as a living password. Telephone call charging without cash, cards or PIN numbers. Ticket less air travel. Premises access control (home, office, laboratory etc.). Driving licenses and other personal certificates. Entitlements and benefits authentication. Forensics, birth certificates, tracking missing or wanted person Credit-card authentication. Automobile ignition and unlocking; anti-theft devices. Anti-terrorism (e.g.: suspect Screening at airports) Secure financial transaction (e-commerce, banking). Internet security, control of access to privileged information. Biometric key Cryptography for encrypting/decrypting messages

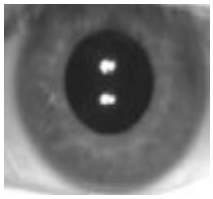
[V] IRIS RECOGNITION SECURITY CHALLENGES

Every biometric technology has its own challenges. When reviewing test results, it is essential to consider the environment and protocols of the test. Much industry testing is performed in laboratory settings on images acquired in ideal conditions. Performance in a real world application may result in very different performance as there is a learning curve for would-be user of the system and not every candidate will enroll properly or quickly the first time. There are some issues which affect the functionality and applicability of iris recognition technology in particular.

[VI] IMPLEMENTATION OF CRYPTOGRAPHY IN IRIS RECOGNITION SYSTEM

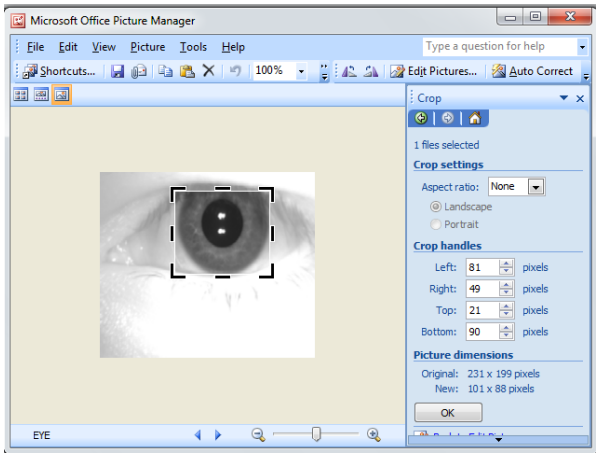
Step 1: Acquisation of image of iris: Scan the image of eye or take it by digital camera

Step2: Before comparison we crop image of eye



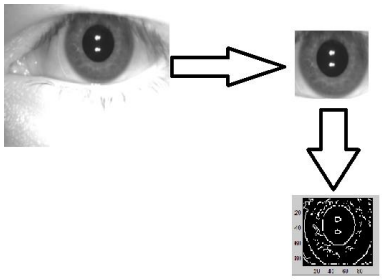
To crop the image of eye we may use photoshop or picture package manager

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 03 | 22 | April-June 2016
Paper is available at www.jrps.in | Email : info@jrps.in



Step 2

After cropping eye edge are detected



Step 3

Store image as matrix in i

>>i=imread('eye1.jpg')

Step 4

Apply canny to i matrix and store in ii

>> ii=canny(i,1,1,1)

Step 5

Now Encrypt the image ii using encryption code in Matlab.

```
function BitCount=encry_coding8(fp,symbol,symbol_count,coding_pattern,sdc,sac,BitCount)%%% Variable Length Coding.

for ii=1:64
   if(coding_pattern(ii)==0)
      %%% DC Coding.
      if(symbol(coding_pattern(ii)+1,2)==0)
         category=1;
      else

category=floor(log10(abs(symbol(coding_pattern(ii)+1,2)))/log10(2))+2;
      end
      FLength=sdc(category).dclength;
      CLength=sdc(category).codelen;

BaseCode=int2bin(symbol(coding_pattern(ii)+1,2),FLength-CLength);

CodedData=strcat(sdc(category).dccode,BaseCode);
      fprintf(fp,'%s',CodedData);
      BitCount = BitCount + FLength;
      CodedData='';
   elseif(coding_pattern(ii)+1 <= symbol_count)
      %%% AC Coding.
      acrun=symbol(coding_pattern(ii)+1,1); %% AC Runlength.
      if(symbol(coding_pattern(ii)+1,2)~=0)  %% AC Non-Zero Integer.
         if(acrun < 16)
            %%% To code Non-zero Integer.

category=floor((log10(abs(symbol(coding_pattern(ii)+1,2)))/log10(2)))+2;
            index=acrun*10+category;
            CLength=sac(index).aclength;
            FLength=CLength+category-1;

BaseCode=int2bin(symbol(coding_pattern(ii)+1,2),FLength-CLength);

CodedData=strcat(sac(index).accode,BaseCode);
            fprintf(fp,'%s',CodedData);
            BitCount = BitCount + FLength;
            CodedData='';
            acrun=0;
         end
      else
         if(acrun==16)
            %%% Special case: To code run of 15+1=16 zeros.
            category=0;
            index=(acrun)*10+2;
            CLength=sac(index).aclength;
```

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 03 | 22 | April-June 2016
Paper is available at www.jrps.in | Email : info@jrps.in

```
            FLength=CLength+category;
            fprintf(fp,'%s',sac(index).accode);
            BitCount = BitCount + FLength;
            CodedData='';
            acrun=0;
          elseif(acrun==17)
            break;   %% symbol(ii,2)==0 ->
symbol(ii,1)=acrun=17, Add EOB.
          end
        end
    end
end

%%% EOB; when acrun = 17 make EOB.
% acrun1=acrun;
acrun=0;category=0;
index=acrun*10+category+1;
CLength=sac(index).aclength;
FLength=CLength+category;
fprintf(fp,'%s',sac(index).accode);
BitCount = BitCount + FLength;
CodedData='';
```

Encoded file

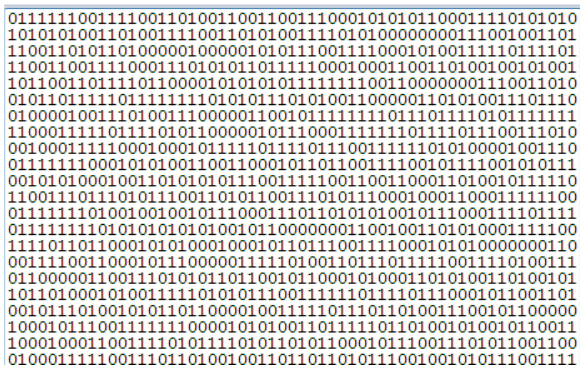


Fig 3 Encoded file

[X] FUTURE SCOPE

In future iris recognitions process is found most secure as compared to other biometric techniques so the security of image base is must. It may be useful to enhance secure transaction in banks and other financial organization. However there are many challenges in frequent use of this technology but in future due to advent of new technology it would be possible to use this technology easily. Enterprise and government both acknowledge the convergence of physical and information security environments, but there are new security challenges on the horizon - just-in-time inventory control, sophisticated supply chain management, and even a phenomenon called "coopetition"-in which companies that compete in some areas, cooperate in others. Managing this convergence of physical and information security requirements now drives security system architecture design and implementation, and is an increasingly key factor in biometric technology selection. Managing convergence will only become a more complex task because as the IT and communications becomes increasingly wireless, the need for robust identity management will become more acute. Iris ID sees iris technology as a natural "fit" for in the physical, infosec, and wireless arenas. We envision a day when iris recognition technology will be deployed in ways that eliminate fraud, provide non-repudiation of sales, authenticate funds transfers, provide signature verification, credit card authorization, and authorized access to healthcare records, intellectual property, and so much more. This growing need, as well as Iris ID competence in iris technology, coupled with core interests in IT and wireless, provides the impetus for design efforts for the future - and makes Iris ID the one to watch for new developments in identity management tomorrow and beyond.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: A Tool for Information Security", IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, 2006, pp. 125-143.

[2] J. Daugman, "New Methods in Iris Recognition", IEEE Trans. on Systems, Man, and Cybernetics, Vol. 37, No. 5, 2007, pp. 1167-1175.

[3] R. Wildes, "Iris Recognition: an Emerging Biometric Technology", Proceedings of the IEEE, Vol. 85, No. 9, 1997, pp. 1348-1363.

[4] W. Boles, and B. Boashash, "A Human Identification Technique Using Images of the Iris and Wavelet Transform", IEEE Trans. on Signal Processing, Vol. 46, No.4, 1998, pp. 1185-1188.

[5] W. Kong, and D. Zhang, "Accurate Iris Segmentation Based on Novel Reflection and Eyelash Detection Model", in International Symposium on Intelligent Multimedia, Video and Speech Processing, 2001, pp. 263-266.

© INTERNATIONAL JOURNAL FOR RESEARCH PUBLICATION & SEMINAR
ISSN: 2278-6848 | Volume: 07 Issue: 03 | 22 | April-June 2016
Paper is available at www.jrps.in | Email : info@jrps.in

[6] L. Ma, and T. Tisse, "Personal Recognition Based on Iris Texture Analysis", IEEE Trans. on PAMI, Vol. 25, No. 12,2003, pp. 1519-1533.

[7] N. Schmid, M. Ketkar, H. Singh, and B. Cukic, "Performance Analysis of Iris Based Identification System the Matching Scores Level", IEEE Transactions on Information Forensics and Security, Vol. 1, No. 2, 2006, pp. 154-168.

[8] V. Dorairaj, A. Schmid, and G. Fahmy, "Performance Evaluation of Iris Based Recognition System Implementing PCA and ICA Encoding Techniques", in Proceedings of SPIE, 2005, pp. 51-58.

[9] C. Fancourt, L. Bogoni, K. Hanna, Y. Guo, and R. Wildes, and N. Takahashi, and U. Jain, "Iris Recognition at a Distance", in Proceedings of the International Conference on Audio and Video-Based Biometric Person Authentication, 2005, pp. 1-13.