ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Visual Cryptography for Biometric Privacy

D.Rajapriya[1], Kanagaraj.N[2], Vignesh Kumar.V[2], Sankar Ganesh.R[2]

Assistant Professor, Department of CSE, RVS Technical Campus, Coimbatore, India[1]

UG Scholar, Department of CSE, RVS Technical Campus, Coimbatore, India[2]

ABSTRACT: Preserving the privacy of digital biometric data (e.g., face images) stored in a central database has become of paramount importance. This work explores the possibility of using visual cryptography for imparting privacy to biometric data such as fingerprint images, iris codes, and face images. In the case of faces, a private face image is dithered into two host face images (known as sheets) that are stored in two separate database servers such that the private image can be revealed only when both sheets are simultaneously available; at the same time, the individual sheet images do not reveal the identity of the private image. A series of experiments on the XM2VTS and IMM face databases confirm the following: 1) the possibility of hiding a private face image in two host face images; 2) the successful matching of face images reconstructed from the sheets; 3) the inability of sheets to reveal the identity of the private face image; 4) using different pairs of host images to encrypt different samples of the same private face.

KEYWORDS: De-identification, Visual-cryptography, Fingerprint, privacy ,Pixel-sharing.

I. INTRODUTION

Modularity (in both program and data) and the concept of abstraction enable the designer to simply and reuse software components. Refinement provides a mechanism for representing successive layers of functional detail. Program and data structure contribute to an overall view of software architecture, while procedure provides the detail necessary for algorithm implementation. Information hiding and functional independence provide heuristics for achieving effective modularity. Software designer develops their project based on their fundamental concept. With several foundation the sophisticated design methods can be applied it is inconceivable that the design of a new machine, new computer chip or a new offline building would be conducted without defining design measures, determining metrics for various aspects of design quality.

II. OVERVIEW

INPUT DESIGN:

The input design is the link that ties the information system into the world of its users. It is a process of converting user-originated inputs to a computer-based format. Input data are collected and organized into a group of similar data. Once identified, appropriate input media are selected for processing.

The goal of designing input data is to make entry easy, logical and free form errors. In input data design, we design source document that capture the data and then select the media used to enter them into the computer. The input forms are developed in a user-friendly way so that a layman also can easily understand everything. Menus are provided to users and different icons are designed so the proposed system design looks decorative. Input design is the part of the overall system design.

Source documents initiate a processing cycle as soon as they are entered into the system through the keyboard. A source should be logical and easy to understand.

Objectives of Input Design:

To achieve the highest possible level of accuracy.

To ensure that the input is acceptableandunderstood by the user.

OBJECTIVES:

1. Enrollment

Enrollment is used to attach image to the process. This contains two forms. They are

New Enrolment

New Enrolment is used to attach the new image to the module

View Enrolment

DOI: 10.15680/IJIRCCE.2016. 0404004

View enrolment is used to view the enrolment image in the screen.

IMAGE SHARING:

Enrol image share creation this form contains the Enrolled image, shared image1 and shared image2 from the shared image create secret shared and then save the secret shared image

IMAGE EXTRACT:

Image Extract is used to view the shared images 1 and 2 from that we can extract the image.

IMAGEVERIFY:

Image Verify is used to view Authentication image and the original Image in this form

III. OUTPUT DESIGN

Output design is very important concept in the computerized system, without reliable output the user may feel the entire system is unnecessary and avoids using it. The proper output design is important in any system and facilitates effective decision-making. The output design of this system includes various reports.

Computer output is the most important and direct source of information the user. Efficient, intelligible output design should improve the system's relationships with the user and help in decision making. A major form of output is the hardcopy from the printer.Output requirements are designed during system analysis. A good starting point for the output design is the data flow diagram. Human factors reduce issues for design involved addressing internal controls to ensure readability.An application is successful only when it can provide efficient and effective reports. Reports are actually presentable form of the data. The report generation should be useful to the management for future reference. The report is the main source of information for user's operators and management. Report generated are a permanent record of the transaction occurred. After any valid transactions; have commenced the report of the same are generations and: filed for future reference. Great care has been taken when designation the report as it plays an important role in decision-marking.

Output forms are also designed in a specific manner as per the user requirement. Results are formatted to enhance clarity. Depending on the user the system would generate appropriate output. The output forms are designed in such a way that the entire user required data is presented.

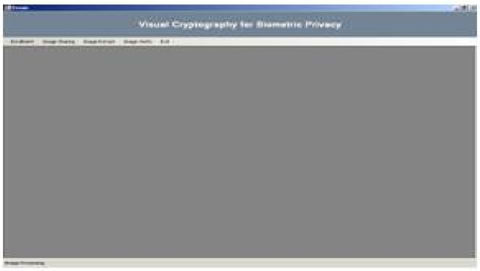
While designing an output, the system analyst must accomplish the following.

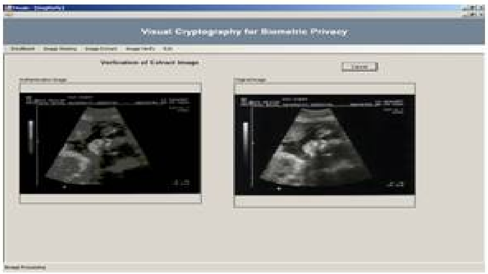
- Determine what information to present
- Decide whether to display, print or speak information and select the output medium.
- Arrange the presentation of information in an acceptable form.
- Decide how to distribute the output to intended users.

Output from computer system is required primarily to communicate the results of processing to users (sometimes to other systems including machine based systems). There are various types of output required by most systems, like

External output whose destination is outside the organization and which require special attention because the project shows the image of the organization.

- **Internal output** whose destination is within the organization and which requires careful design because they are the users main interface with the computer.
- **Operational output** whose uses purely within the department.
  - **Interactive output**, which involves the user in communicating directly with the computer.
  - **Turn around output** i.e., re-entered documents to which data will be added before they are returned to the omputer for further processing.



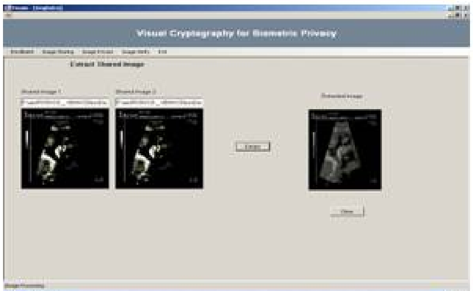

Visual Cryptography for Biometric Privacy
Verification of Extract Image

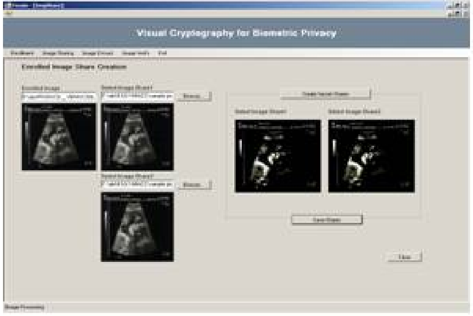
ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

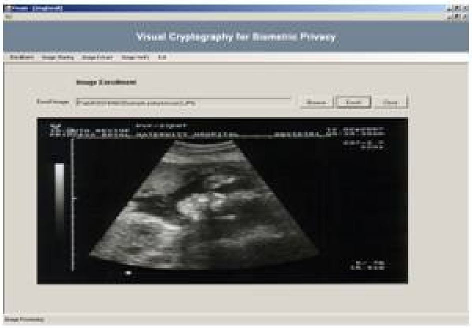
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016




Visual Cryptography for Biometric Privacy
Enrolled Image Share Creation



IV. MODULES

- Biometric data enrolment
- Share Creation
- Image Restoration
- Image verification

2.2MODULE DESCRIPTION:

2.2.1Biometric Data Enrollment:

The biometric data(image) is stored to image database.The template of a person in the database is generated during enrollment and is often stored along with the original raw data.During the enrollment process, the private biometric data is sent to a trusted third-party entity. Once the trusted entity receives it, the biometric data is decomposed into two images and the original data is discarded.

2.2.2Share Creation:

For each image a set of two candidate images are chosen to be used as shares. The pixels of the chosen images are manipulated at two subpixel block level with the original image ans stored as two shares. The decomposed components are then transmitted and stored in two different database servers such that the identity of the private data is not revealed to either server.

2.2.3Image Restoration:

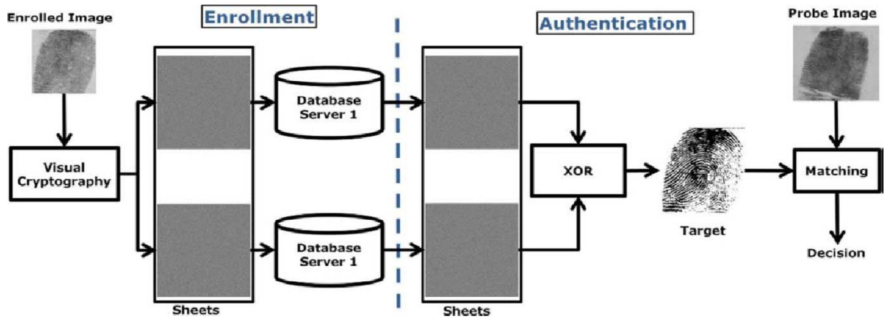
During the authentication process, the trusted entity sends a request to each server and the corresponding sheets are transmitted to it. Sheets are overlaid (i.e., superimposed) in order to reconstruct the private image thereby avoiding any complicated decryption and decoding computations that are used in watermarking, steganography , or cryptosystem approaches. Once the matching score is computed, the reconstructed image is discarded. Further, cooperation between the two servers is essential in order to reconstruct the original biometric image. The XOR operation is applied on the two share images to retrieve the original image.

2.2.4Image Verification:

The retrieved image is verified against the original image. We choose a threshold value of the desired verification range. For high accuracy systems, we can choose a high threshold value and for simple systems, we can choose a medium threshold value. Based on the match, the retrieved image is concluded to either match or not match the original image.

DOI: 10.15680/IJIRCCE.2016. 0404004

2.3EXISTING SYSTEM MODEL:

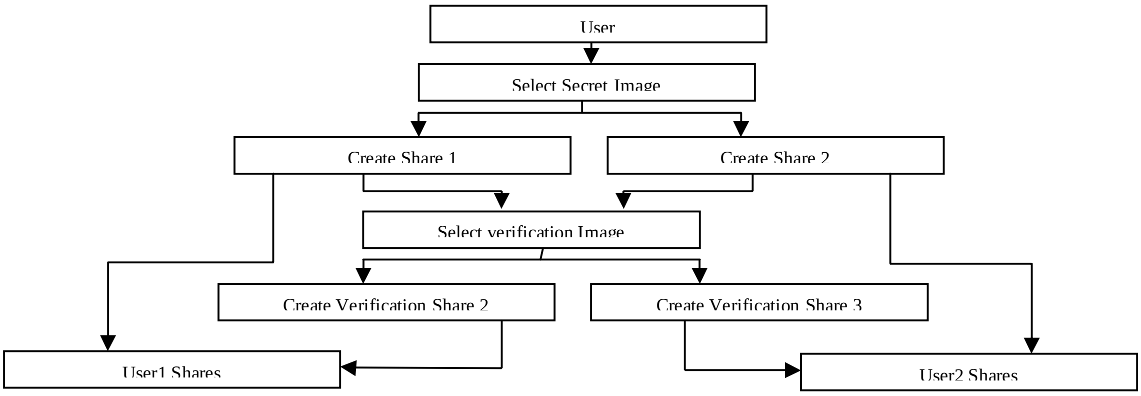


4.1 SYSTEM FLOW DIAGRAM:

The System flow diagram is the way of expressing system requirements in a graphical form. It is also known as bubble chart. It has the purpose of clarifying system requirements and identifying major transformations that will become programs in system design. It is the starting point of the design phase that functionally decomposes the requirements specifications down to the lowest level details.The SFD may be used to represent the system or software at any level. A level of SFD also called model represents the entire software element as a single bubble with input and output arrows.

A SFD consists of a series of bubbles joined by lines. The bubbles represent data transformations and the lines represent data flows in the system. SFD typically shows minimum content of data stores. Each data store should contain all data elements that flow in and out. The SFD methodology is quite effective. Especially when the required design is unclear and the analyst need a notational language for communication. The SFD is easy to understand after brief orientation.

System Flow Diagram – Encoding Process:


User
Select Secret Image
Create Share 1
Create Share 2
Select verification Image
Create Verification Share 2
Create Verification Share 3
User1 Shares
User2 Shares

V. SYSTEM TESTING AND IMPLEMENTATION

5.1 SYSTEM TESTING:

5.1.1 Testing Methodologies:

Testing is a process used to help identify the correctness, completeness and quality of developed computer software. There are many approaches to software testing, but effective testing of complex products is essentially a process of investigation, not merely a matter of creating and following rote procedure. One definition of testing is "the process of questioning a product in order to evaluate it", where the "questions" are things the tester tries to do with the product, and the product answers with its behavior in reaction to the probing of the tester.

The quality of the application can and normally does vary widely from system to system but some of the common quality attributes include reliability, stability, portability, maintainability and usability.

Testing objectives include
1.Testing is a process of executing a program with the intent of finding an error.
2. A good test case is one that has a high probability of finding an as yet undiscovered error.
3. A successful test is one that uncovers an as yet undiscovered error.

Testing should systematically uncover different classes of errors in a minimum amount of time and with a minimum amount of effort. A secondary benefit of testing is that it demonstrates that the software appears to be working as stated in the specifications. The data collected through testing can also provide an indication of the software's reliability and quality. But, testing cannot show the absence of defect -- it can only show that software defects are present.

5.2Black box testing:

Black box testing attempts to derive sets of inputs that will fully exercise all the functional requirements of a system. It is not an alternative to white box testing. This type of testing attempts to find errors in the following categories:

1. incorrect or missing functions,
2. interface errors,
3. errors in data structures or external database access,
4. performance errors, and
5. initialization and termination errors.

5.3White box testing:

This testing is based on knowledge of the internal logic of an application’s code. Also known as Glass box Testing. Internal software and code working should be known for this type of testing. Tests are based on coverage of code statements, branches, paths,conditions.White box testing is a test case design methodthat uses the control structure of the procedural design to derive test cases. Test cases can be derived that

1.Guarantee that all independent paths within a module have been exercised at least once.
2.Exercise all logical decisions on their true and false sides,
3.Execute all loops at their boundaries and within their operational bounds, and
4.Exercise internal data structures to ensure their validity.

5.4Quality Assurance:

5.4.1Generic risks:

A risk is an unwanted event that has negative consequences. Project managers will engage in risk management to understand and control the risks on their projects. We can distinguish risks from other project events by looking for three things.

- A loss associated with the event
- The likelihood that the event will occur
- The degree to which we can change the outcome

The generic risks such as the Product size risk, Business impact risks, Customer-related risks, Process risks, Technology risks, Development environment risks, Security risks etc. for this project are analyzed and documented by the senior staffs in the organization. This project is developed by considering these issues and with the constant support from senior staffs in the organization.

5.4.2Security Technologies & Policies:

A computer-base system is a combination of many assets or resources designed to perform some function or to provide some services.Each of these assets is threatened by one or more of the following unacceptable events:

- Interruption
- Disclosure
- Removal
- Destruction
- Security Issues

The term security can be divided into four related issues

- Security
- Integrity
- Privacy
- Confidentiality
- Authentication

DOI: 10.15680/IJIRCCE.2016. 0404004

In the system brief log on procedure for the customer was provided in order to enter and accessthe system. This process is done in order to identify the valid user.

These attributes are stored in a table that cannot be easily trapped by unauthorized persons.

5.4.3 File protection:

The various files and database tables are also highly secured in this system. The necessity for securing the files and the table evolves because some persons who were not given authorization for access may hacker files and corrupt the tables with wrong data which will response tremendous hazards to the operations of the system. So in order to avoid these things,the data encryption standards engine is attached to all files and database tables associated with the system,which will facilitate encryption and decryption of files. Backup of the system are also taken as a preventive measure.

VI. CONCLUSION

This software provides a user – friendly approach towards the system. This system has been well developed and when implemented, is bound to satisfy all of the requirements. Painstaking efforts have been taken to make the software impeccable and upgradeable. There is a hope that this software will be utilized to its maximum and will do a good job in long run.

The ubiquitous nature of change underlies all software work. Therefore, we must develop mechanism for evaluating, controlling and making modification. This project has been created using the best design and coding technique known. It can be migrated to new platforms, adjusted for changes in machines and operating system technology and enhanced to meet now user needs, all without regard to overall architecture.

The efficiency of the application lies in the hands of the end – users. Care has been taken to provide this user friendly system so that not only the experienced and professional agents use the system but will prove useful for the new agents also. The visual cryptography for biometric privacy has been developed for encoding the secret images. It also allows the user to decode the image. Thus this project provides an easy way in hiding the images.

VII. SCOPE FOR FUTURE ENHANCEMENT

The growth of any organization leads to enhancements, in future the system can be enhanced according to requirements. In order to become an effective system, the developed system should provide room for improvement and enhancement.**Visual Cryptography for biometric privacy** is designed and developed flexibly according to the current requirements of the user The requirements may increase in future and the system can be easily modified accordingly as the system has been modularized. The system is developed in such way that any future developments can be included.Future development may be made in the direction of making the system as the decision support system.

REFERENCES

[1] A. Jain, P. Flynn, and A. Ross, Handbook of Biometrics. New York: Springer, 2007.

[2] M. Naor and A. Shamir, “Visual cryptography,” in Proc. EUROCRYPT,1994, pp. 1–12.

[3] G. I. Davida, Y. Frankel, and B. J. Matt, “On enabling secure applications through off-line biometric identification,” in Proc. IEEE Symp.Security and Privacy, 1998, pp. 148–157.

[4] B. Thuraisingham and W. Ford, “Security constraint processing ina multilevel secure distributed database management system,” IEEETrans. Knowl. Data Eng., vol. 7, no. 2, pp. 274–293, Apr. 1995.

[5] M. Nakajima and Y. Yamaguchi, “Extended visual cryptography fornatural images,” J. WSCG, vol. 10, no. 2, pp. 303–310, 2002.

[6] C. Soutar, D. Roberge, A. Stoianov, R. Gilroy, and B. Kumar, “Biometric encryption,” in ICSA Guide to Cryptography. New York: Mc-Graw-Hill, 1999.

[7] A. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,”EURASIP J. Advances Signal Process., pp. 1–17, 2008.

[8] Y. Rao, Y. Sukonkina, C. Bhagwati, and U. Singh, “Fingerprintbased authentication application using visual cryptography methods (improved ID card),” in Proc. IEEE Region 10 Conf., Nov. 2008, pp.1–5.