


E-Sign Detector: Image Steganography-Based Employee Identification System E-Sign Detector: Image Steganography- ...

Vijay Senthoo

Related papers

[Download a PDF Pack](#) of the best related papers 



[Insider Threat - Protecting The Enterprise From Sabotage, Spying, And Theft](#)

Isromi Janwar

[A Secured Smart Card using a Pseudorandom Affine Transformation Based Cipher and a Secured LIR...](#)

Ehab Mahmoud Mohamed

E-Sign Detector: Image Steganography-Based Employee Identification System

V Senthooan*, M T Chathuranga** and T Kartheeswaran***

This paper aims to develop a desktop application system called E-Sign detector using image steganography. It targets to fulfill the requirements of small and medium size companies to identify their employees through a specially designed embedded picture employee ID card. This employee ID card will be able to track the employee when he/she is attempting to enter through a doorway of the company. Hence, this will be highly advantageous for small companies where it is needed to grant special privileges to a certain number of officers to enter a high defensive area. This application will be a real-time system with higher reliability that saves time and decreases the manpower usage and provides higher security. Through this system, the company can mark the time at which an employee is accessing a certain place and leaving that place, and maintain daily attendance automatically. Finally, we argue that the proposed system will be a good substitution for the replacement of manual employee identification system as we have implemented and solved the drawbacks found in a manual employee identification system.

Keywords: Image steganography, Employee ID, Cryptography, LSB, Encryption, Decryption

Introduction

There was an era when almost all the works in an organization such as marking the attendance of the employees, salary calculation, management, sharing ideas and passing information were done manually. However, those who have been a part of the company when attendance registers were used know how easy it was to abuse such a method of attendance and mark bogus attendances for each other (Kristin Finklea, xxxx). Of course, technology had to play its role in this field just as well as it had done in other fields. The employee identification system is created and it changed the way attendances were marked. This software deals with desktop environment for identifying the employees of a company, organization or any other workplace automatically and is known as E-SIGN Detector. This project provides solutions for the problems regarding a workplace where employee identification is necessary and higher security is important. The system can identify the user simply by the employee identification card issued for each employee of the workplace. This software is specially designed for the working

Author please provide the year

please confirm the authors information

- * Lecturer, Department of Physical Science, Vavuniya Campus, University of Jaffna, Sri Lanka, and is the corresponding author. E-mail: senthooan@mail.vau.jfn.ac.lk and vijaysenthoor@gmail.com
- ** Undergraduate Student, Department of Physical Science, Vavuniya Campus, University of Jaffna, Sri Lanka. E-mail: mthilinachathuranga@gmail.com
- *** Lecturer, Department of Computer Science and Technology, Uva Wellassa University, Badulla, Sri Lanka. E-mail: tkarthees@gmail.com

pl chk two email ids

environments where security is one of the most important factors to be considered. This piece of work is capable of detecting the arrival and leaving of a certain employee to a certain place and to grant access/permission to a certain employee to a certain area of a workplace as necessary and as privileged by the company administration previously.

The manual file processing system was observed by using some organizations and companies in some of the districts in Sri Lanka to monitor the attendance of employees.

- Post Offices
- Education Offices
- Garments Shops
- Campuses

Although some of the activities inside these organizations are computerized, still they are using a log book to keep records regarding employee attendance. Due to several reasons, these manual records are not trustworthy. Some of the drawbacks of the manual file processing system in these organizations are:

- Inconsistency of data
- Data repetition
- Inefficiency
- Ambiguousness
- Inconvenience

Apart from those drawbacks, with the frequently happening human-made mistakes, most of the data found in manual systems become unreliable. This would cause data dissatisfaction within the company. To overcome these existing problems, our proposed system provides the following benefits to users in small organizations:

- It provides a fast, reliable, secure and real-time system to identify a certain employee in a simpler manner.
- It helps the company to mark the daily attendance of employees and calculate working hours, and also leave taking and salary calculation.
- It enables the ability to grant access permission for genuine and authorized staff members to enter high defensive areas of the company. This will ensure the security of company hubs and the security of confidential information/data, stores, etc.
- Even though we cannot claim that this work is entirely a masterpiece or an exhaustive piece of work, the main purpose of the effort is to detect the employee through an automated system rather than the manual record-keeping system which is unnecessarily time-consuming and requires human effort.

We assure that this software can be used easily by even a non-programming personal, avoiding the chance of error. This application provides two modules. They are administrative module and user module.

Using the administrator module, the user can

- Login
- Check employee details
- Check decoding and identification process
- Update/alter employee details
- Create Embedded ID cards
- Register employees

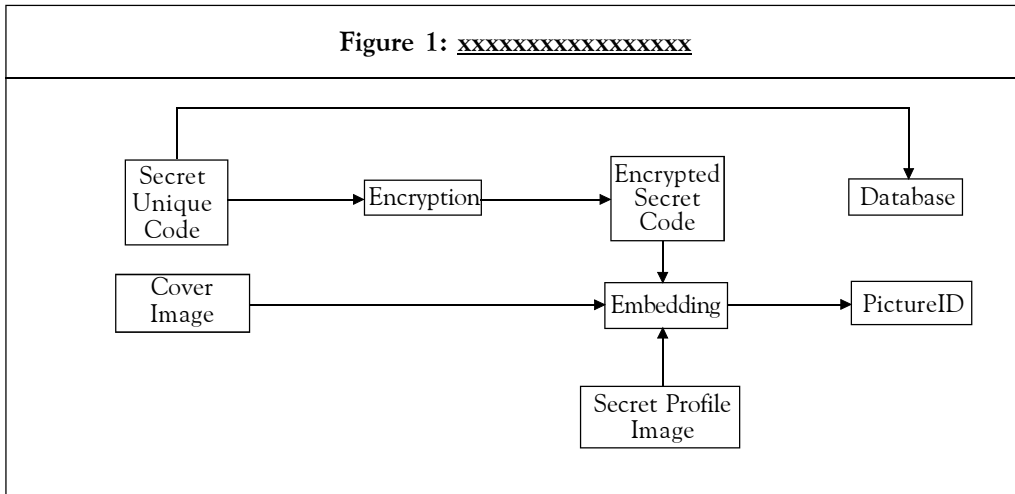
Using the user module, the user can get access permission to a certain area of the company premises as necessary. Thus, E-Sign detector provides the automation of the process of employee detection and granting access permission to the employee as necessary. Steganography is the art of hiding a message within another so that the hidden message is indistinguishable (Parmar and Krishna, 2015). The key concept behind steganography is that the message to be transmitted is not detectable to casual eyes. Text (Hu *et al.*, 2011), image (Chen *et al.*, 2003), video (Bender *et al.*, 1996) and audio (Kartheswaran *et al.*, 2015) are used as a cover media for hiding data in steganography. In text steganography, message can be hidden by shifting word and line, in open spaces and in word sequence (Bennet, 2004-2013). The properties of a sentence such as number of words, number of characters, number of vowels and position of vowels in a word are also used to hide secret message. The advantage of preferring text steganography over other steganography techniques is its smaller memory requirement and simpler communication (Bennet, 2004-2013). Visual Cryptography (VC), proposed by Naor *et al.* in (Bennet, 2004-2013), is a cryptographic technique based on visual secret sharing used for image encryption. Using k out of n (k, n) visual secret sharing scheme, a secret image is encrypted along with meaningless images that can be transmitted or distributed over an untrusted communication channel. Only combining the k shares or more gives the original secret image.

2. System Overview

2.1 System View: Encryption

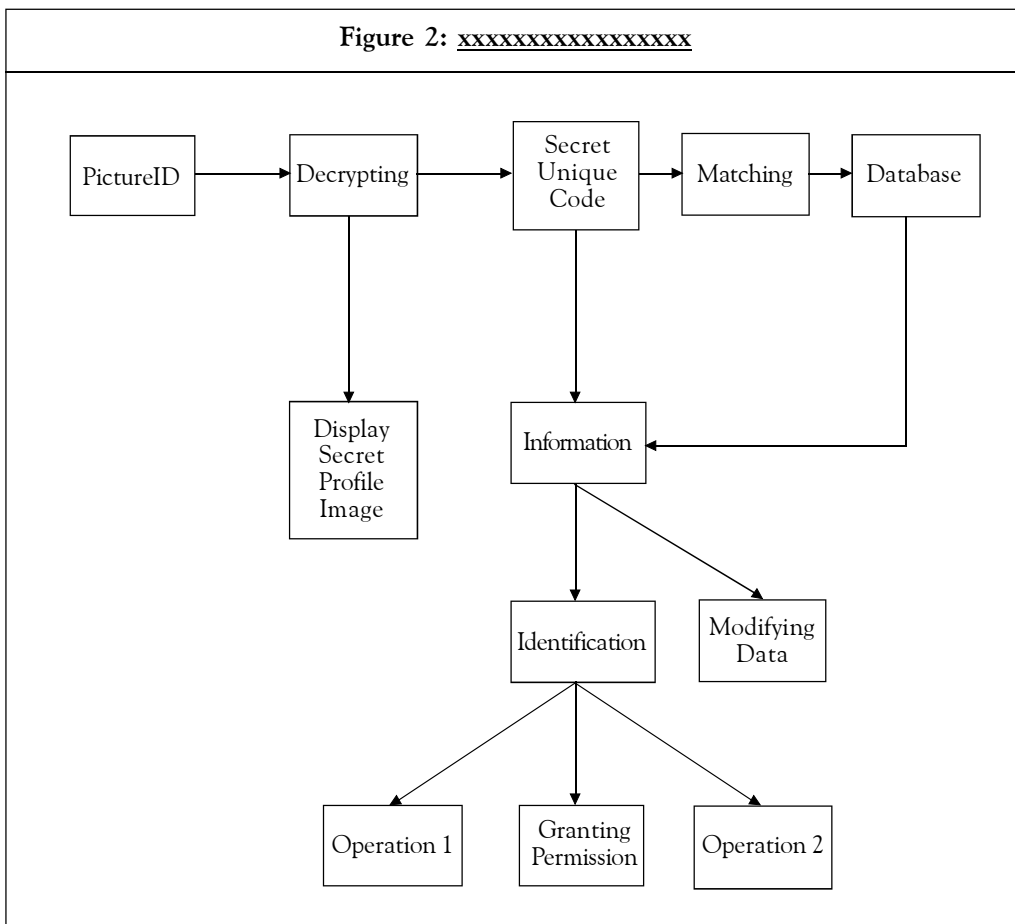
The encrypted secret unique code and secret profile image are embedded with the cover image and generated as an employee picture ID. The secret unique code is stored at the database. After the web camera or other devices scan the picture ID, the system will decrypt the secret unique code and secret profile image and then display the profile image. The secret unique code is matched with the database and will give the information about the particular employee. Then the employee can be identified as the authorized employee of the organization. After that, the permission will be granted to that employee and some operations can be made.

Author, please cite all figure numbers in text at appropriate place and provide headings



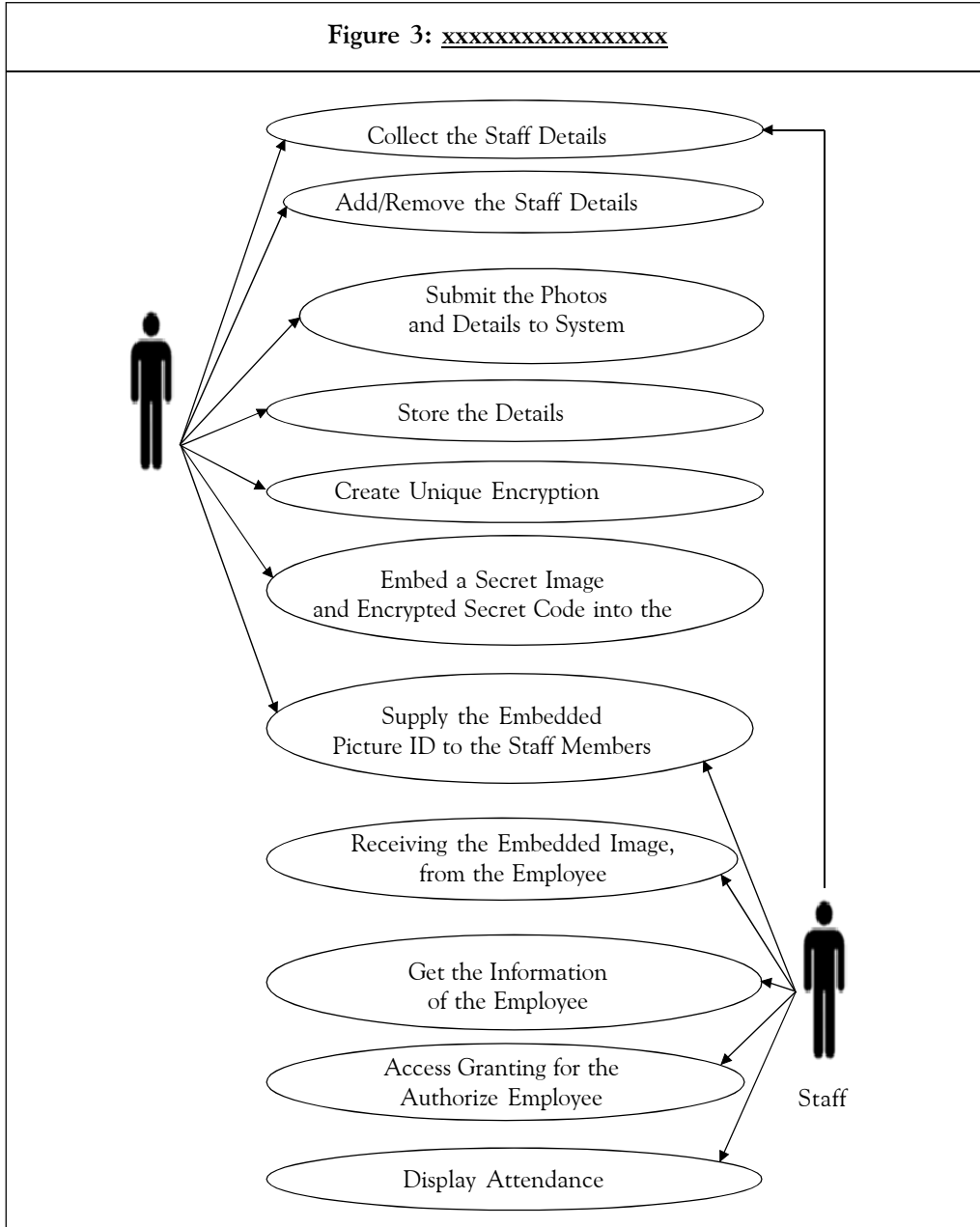
2.2 System View: Decryption

Author, Heading to be provided



2.3 Usecase Diagram

Author,
Heading to be
provided



3. Methodology

3.1 Requirements Collection

Search and collect the data from some organization which is using manual attendance system in Vavuniya district by having conversations with the HR department of

organization to know about the daily attendance of employees and also the problems faced in the manual system of attendance.

- Keep each of the organization's employee details such as name, employee no., contact details, salary, duty time, etc.
- Waste of time in manual marking of attendance.
- Inefficiency in salary calculation and other activities.
- Overload of work.
- Duplicate data entry such as faults between each employee.
- Failure in prevention of frauds.

3.2 Proposed Method

With collected requirements, we have developed a software application called as E-Sign-Detector to identify the secret code and the employee profile image which have been hidden in the embedded image, created by the same system, and then it will display the employee's profile image and mark his/her attendance.

The step-by-step procedure is as follows:

Step 1: Identify the problems from gathered requirements in manual attendance maintained in small companies and small organizations.

Step 2: Design a system to solve the problems and develop a software application with appropriate interface design.

Step 3: Encode secret photos and codes to a cover image and create stock of embedded images, exactly same as the cover image.

Step 4: Create the employee ID cards with the embedded images for each employee in organization.

Step 5: Test the software application with appropriate ID card and find the testing results and outputs.

Step 6: Finalize the application for working and publishing.

The process of this application is to recognize the hidden images from embedded images to identify the employees of the company through a specially designed employee ID card. This would help in detecting employee's profile image and secret code from embedded image and display the profile image at that time, matching the secret code with stored code in database, and finally marking the employee attendance.

The focus of application could be divided as follows:

- **Research into the Limitations of the Existing Techniques:** This work is mainly focused on identifying a particular employee profile and code from the embedded image.

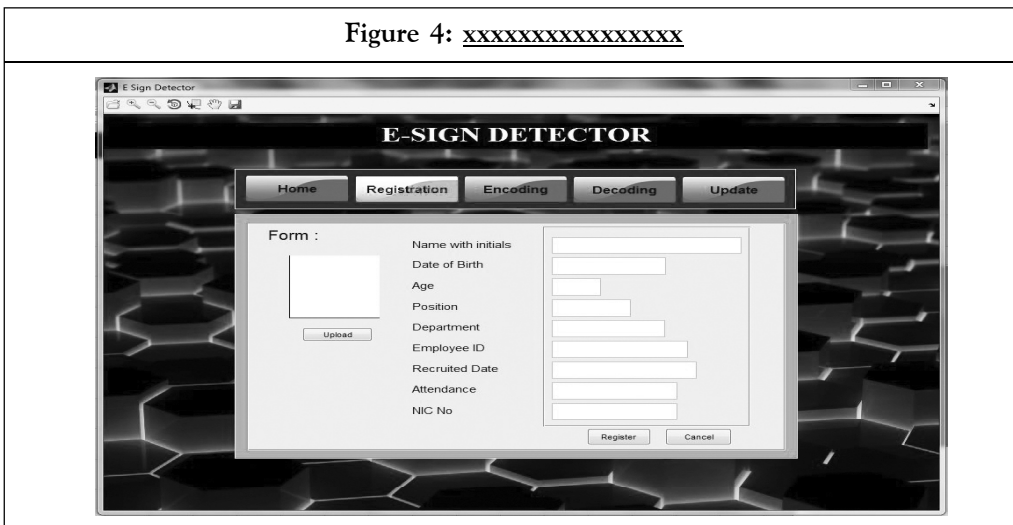
- **Analyzing the Feasible Improvements/Contribution of the Techniques:** We identify the particular hidden profile image from embedded image using the web camera.
- **Testing and Analyzing the System with Multiple Employee ID Card:** This system will capture the profile picture and code of each employee with different employee ID card and will identify fakes.

3.3 User Interfaces

The following tab is for employee details registration. This tab can be accessed only by the administrator. The administrator is privileged to access all the tabs.

Author,
Heading to
be provided

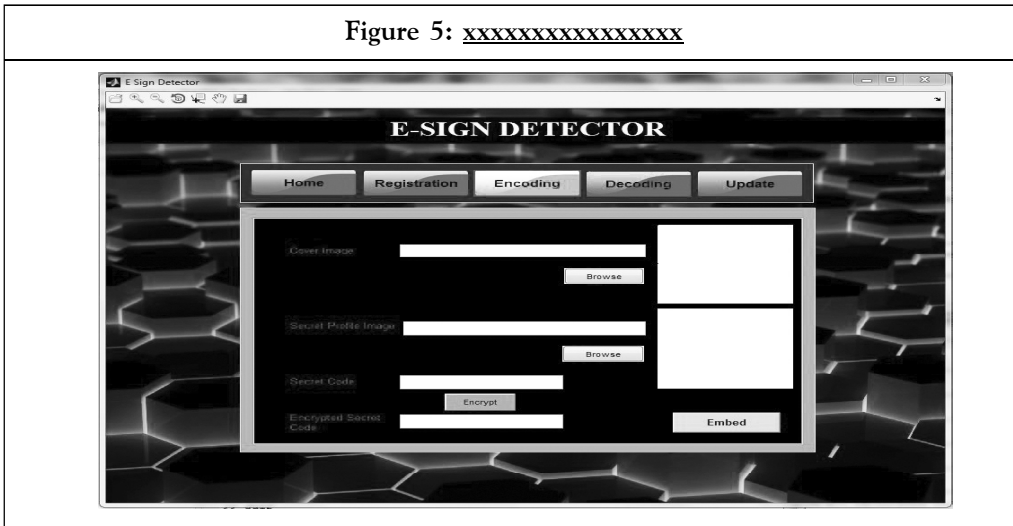
Figure 4: XXXXXXXXXXXXXXXXXX



The following tab is for encoding procedure. This tab can also be accessed only by administrator.

Author, Heading
to be provided

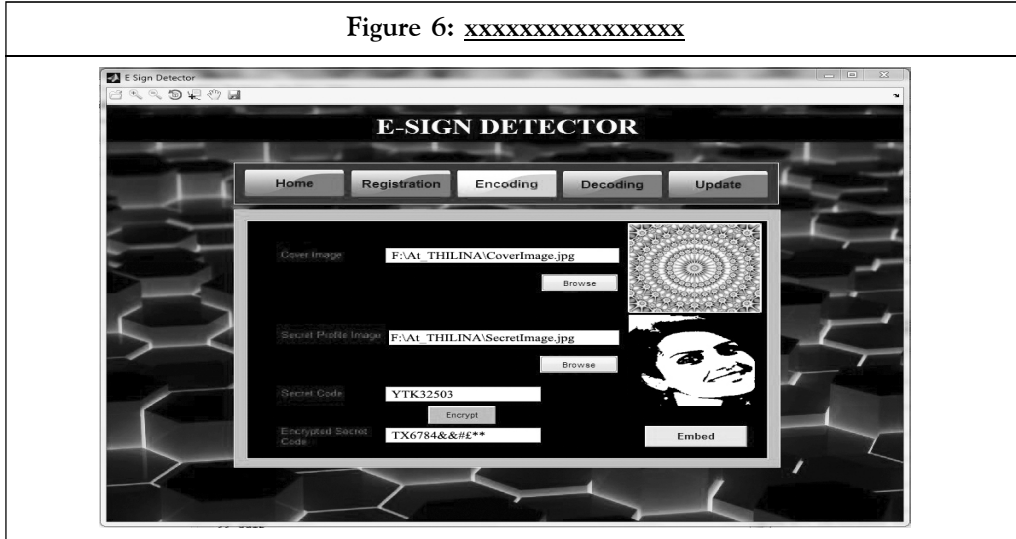
Figure 5: XXXXXXXXXXXXXXXXXX



After filling the details of the employee, the administrator will browse for the original image and the secret image, and then will assign a secret code, press the encrypt button and finally will press the embed button. Then the secret image and the code will be embedded into the original image.

Author, Heading to be provided

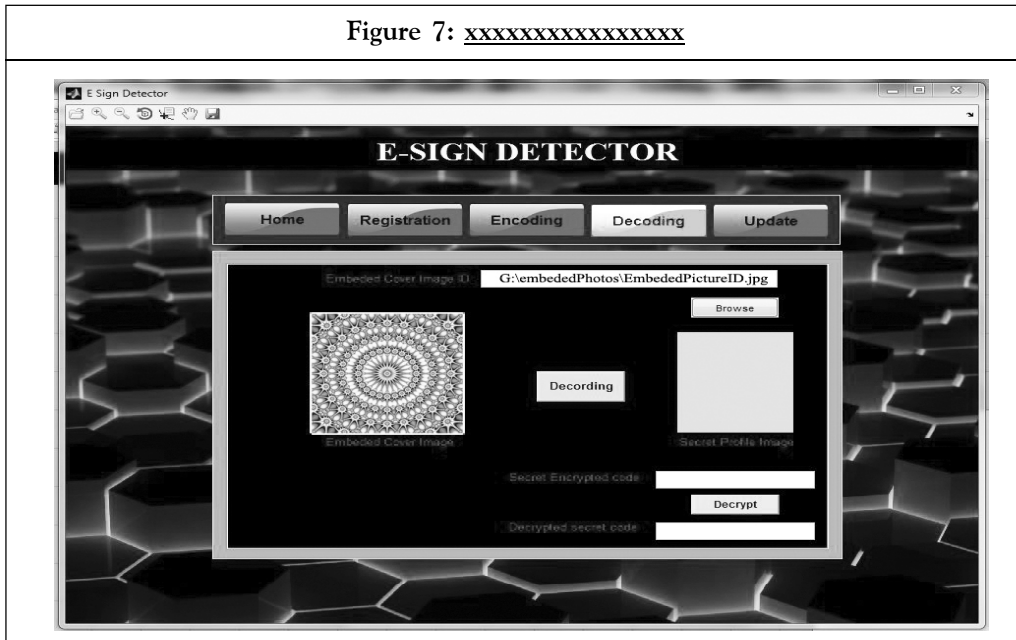
Figure 6: XXXXXXXXXXXXXXXXXXXX



The following tab is for the decoding process. First, the administrator will browse for the embedded image. The image will appear when administrator presses the decoding button, and the secret image and the code will respectively be decoded into the relative spaces.

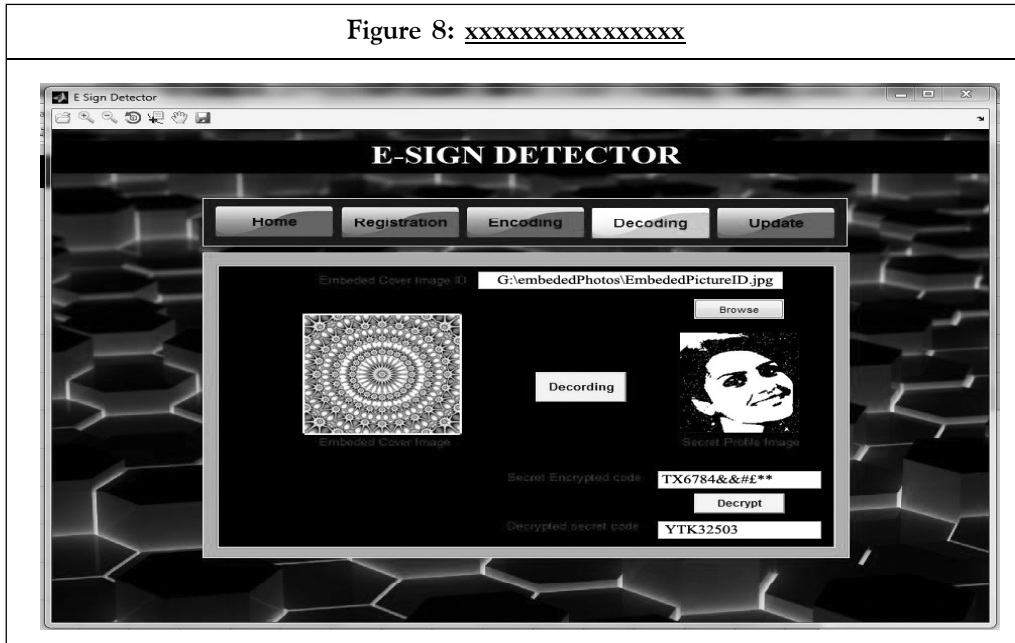
Heading to be provided

Figure 7: XXXXXXXXXXXXXXXXXXXX



The following tab (Figure 8) is the decoded secret image and the decrypted security code.

Heading to be provided



If the security code and embedded image are available and are matching with the database, and if the person is authorized, then the access permission is granted.

Heading to be provided



4. Evaluation and Testing

Software testing is the process of executing a program or system in order to detect errors and see whether it has met its required results. Testing is a process with high importance; hence only by testing we can determine whether we have reached our targets. Testing was done on every version of the system until it was ensured that the final version met the expected objectives.

It involves the execution of a software component or system to evaluate one or more properties of interest. In general, these properties indicate the extent to which the component or system tested:

- Meets the requirements that guided its design and development;
- Responds correctly to all kinds of inputs;
- Performs its functions within an acceptable time; and
- Can be installed and run in its intended environments.

We trust that this software fulfills all the expected requirements. We have performed the testing process by using 20 authorized IDs and 20 fake IDs. This system analyzed the fake IDs and identified that they are fake. But one ID is accepted as authorized ID. For the authorized IDs, our system accepted all the 20 IDs as original and those 20 IDs are belonging to the organization or company. So we can say our project is 97% successful. The differences between this system and other systems are: other systems also capture the image through the same devices like web camera; there also when capturing, the quality of the image is changed due to some reasons; that image is stored in the database and when they match the image another time, it will match without any problems because the new image and the previous image are same in quality (reduced quality). And if the new captured image matches with the previous stored image than given percentage, the other systems are able to identify images easily. But this system needs to identify not only the outlook of the images, but also the hidden data that human eye cannot recognize. It is harder to analyze those modifications as the quality reduction occurred in web cameras or other cameras.

Author,
please check

When we tried to apply the identification process to the scanned images (when scanning through the web camera or other devices), this system cannot identify the modification is made by the algorithm or the quality reduction issues occurred in the procedure of printing and capturing images. But this system algorithm divided the secret image into 4 equal parts, each one with 90 degree angle. The 1st part contains the modified secret image (the modifications are made by the algorithm); The 2nd part contains the original image; and the 3rd part contains the security code. So, both original image and embedded image are designed and stored in this complex photo. So, each time the picture ID is captured by the web camera, both original and embedded parts are affected by the light intensity with same percentage. And that helps the system to get the idea how much of modifications happened due to light intensity. So

we found our own solution, which has never been used in steganography according to our knowledge, to address the light intensity problem.

Conclusion

The E-Sign Detector (Employee Identification System) was created to cater to the needs of some companies which are using manual system for employee identification and attendance marking. Using this manual system they faced problems like work load, salary calculation, waste of time, needing a specific security place for keeping the files and unauthorized access to the restricted area without permission. To overcome all these problems, we created and the proposed system. The system will reduce lots of wastage time and will reduce a number of large logbooks for keeping manual records, and also it will help to maintain the security of high defensive areas. Finally, this system was developed using some techniques. Nowadays, most of the people like to use automation and computerized system. So we hope that everyone will use our system and that small organizations will find it very useful. ☺

References

1. Bender Walter, Gruhl Daniel, Morimoto Norishige and Lu A (1996), "Techniques for Data Hiding", *IBM Systems Journal*, Vol. 35, Nos. 3&4, pp. 313-336.
2. Bennet K (2004-2013), "Linguistic Steganography: Surevey, Analysis, and Robustness Concerns for Hiding information in Text", Purdue University, Cerias Tech Report 2004-2013.
3. Chen J, Chen T S and Cheng M W (2003), "A New Data Hiding Scheme in Binary Image", *Proceeding of Fifth International Symposium on Multimedia Software Engineering*, pp. 88-93.
4. Daniel Gruhl, Anthony Lu and Walter Bender (1996), "Echo Hiding", *Proceedings of the First International Workshop on Information Hidding*, pp. 293- 315, Cambridge, UK.
5. Finklea Kristin (xxxx), *Identity Theft: Trends and Issues*, Congressional Research Service, [7-5700 www.crs.gov R40599](https://www.crs.gov/R40599).
6. Hu Sheng Dun and KinTak U (2011), "A Novel Video Steganography Based on Non-uniform Rectangular Partition", *Proceeding of 14th International Conference on Computational Science and Engineering*, Dalian, Liaoning, pp. 57-61,
7. Kartheswaran T, Senthoooran V and Pemedasa T D D L (2015), "Multi Agent Based base Audio Steganography", *IEEE International Conference on Computational Intelligence and Computing Research*, pp. 807-810.
8. Parmar Ajit Kumar Maganbhai and Krishna Chouhan (2015), "A Study and Literature Review on Image Steganography", *International Journal of Computer Science and Information Technologies*, Vol. 6, No. 1, pp. 685-688.

Reference # 35J-2016-06-xx-01

Author check
reference no. 4
not cited in the
text

Author please
provide the year