ISSN: 2521-0874 (Print)
ISSN: 2521-0505 (Online)

Contents List available at RAZI Publishing
Acta Informatica Malaysia(AIM)
Journal Homepage: http://www.razipublishing.com/journals/acta-informatica-malaysia
https://doi.org/10.26480/aim.01.2017.12.16

Web Based Watermarking System

Mak Kai Shun, Hanayanti Hafit, Shahreen Kasim, Mohd Farhan Md Fudzee, Azizul Azhar Ramli, Hairulnizam Mahdin, Seah Choon Sen

Faculty of Computer Science & Information Technology, Universiti Tun Hussein Onn Malaysia,
Beg Berkunci 101, 86400 Parit Raja, Batu Pahat, Johor Darul Takzim, Malaysia.
kaishun2908.KS@gmail.com, {hana, shahreen, farhan, azizulr, hairuln}@ uthm.edu.my, seanseah0702@gmail.com

ARTICLE DETAILS

Article history:

Received 22 January 2017
Accepted 03 February 2017
Available online 05 February 2017

Keywords:

Claim Management, Mileage Claim, Overtime Work Claim

ABSTRACT

The recent progress in the digital multimedia technologies has offered many facilities in the transmission, reproduction and manipulation of data. However, this advance has brought the problem such as copyright protection for content providers. Watermarking is one of the proposed solutions for copyright protection of multimedia. Most of the content provider use Photoshop to create a watermark photo, but Photoshop involve many procedures to complete a watermarked image. In addition, watermark image using Photoshop easily destroy by attacker where attacker can modifies the image to remove the watermark from the image. Hence, it has become a tough task to protect copyright of an individual's creation. Thus, i-Mark is developed to solve the problem to protect the watermarked image. An invisible watermark embeds an imperceptible signal into data such as image, which indicates whether or not the content is copyrighted. By using i-Mark, invisible watermarking was provided where steganography method was implemented for users to encrypt message into an image. Hence, the image is protected from been easily modifies or copy by others. Meanwhile, i-Mark allow user to store their invisible watermarked image in database and can be view later. In addition, i-Mark also can made a visible watermark where user can adding text on the cover of image more convenient than Photoshop. In conclusion, i-Mark provides users to watermark their image either visible watermark or invisible watermark. Hence, throughout the project, user may use the system user friendly compare to Photoshop.

1. Introduction

Digital Watermarking is vital element in data hiding which can protect copyright content of images. Watermarking is a method for embedding some information into the cover image where the information can be extracted or detected for few purpose such as authentication, owner identification, copyright protection and others [5]. Therefore, the aim of watermarking is to providing security of the digital content.

Watermarks may be visible or invisible to human vision. Visible watermarking refers to the information can be seen on the image. Visible watermarks are typically logos or text. Invisible watermarking refers to adding information that cannot be seen by human vision on an image. It may also be a form or type of steganography and is used for widespread use. Steganography method includes two algorithms: one as the embedding algorithm and other as the detecting algorithm. Figure 1 shows the watermark embedding process into the cover image while Figure 2 shows the watermark detection process.

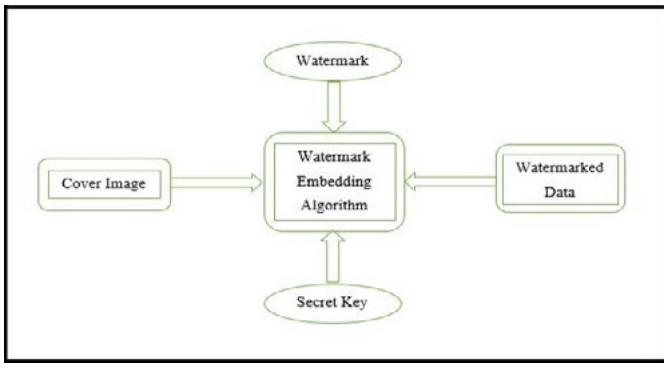

Figure 1: Watermark Embedding Process [6]

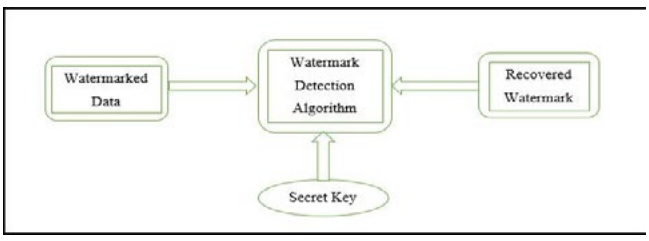

Figure 2: Watermark Detection Process [6]

The following objectives have been determined:

i. To develop a web based watermarking system that can watermark image.
ii. To implement steganography technique into watermarking system.

This system is open for everyone, especially for photographers. Photographers is responsible to their photo by protect the photo. To avoid photo been retrieve by others, photographers could use this watermarking system to make a copyright. Photo taker can use this system to watermark their photo and store the photo after been watermarked. Photo taker may choose visible watermark or invisible watermark in this system.

The reminder of the paper is organized as follows. Part II discuss the literature review conducted on the system to be proposed. Part III describe the methodology to be used for the system development. Part IV describe the implementation and testing of the system. Part V describe about the implementation of actual coding process, algorithm and system testing process to proposed system. Part VI describe about the conclusion of entire project and outline limitation and future work of the proposed system.

2. Literature Review

In this part focus on a relative new field of study in Information Technology known as steganography. Steganography technique was applied into this digital watermarking system (i-Mark).

Digital watermarks have been proposed as a potential method for protection of ownership rights on images. Watermarking can be classified into two types which are visible watermarking and invisible watermarking.

Since the rapid growth of network and ease of media manipulation, it gave rise to problem for instance unauthorized copying and distribution of digital media. Though cryptographic technique is used to prevent from unauthorized access, but it does not prevent authorized user form illegally replicating decrypted content. Hence, watermarking is the effective solution to solve this problem which is to protect copyright and authentication of owner. According to Barni et al., a watermarking application should be robust, so that it can protect the copyright of the owner [2]. According to Alattar, the reversible watermarking method has been proposed in last few years and the extracted watermark can be used as the evidence for author's copyright [1].

A. S-Tool

S-Tools is a free software that works on Windows95 and above. It can hide data in GIF format or .bmp image files or .wav audio files. S-tools also use to compress files. For all file formats that are supported by S-Tools save the data in 3-bits LSB of each byte data.

For image type file, S-Tools work by using LSB technique and depending on the selected file format. Secret data was hidden into the image by using LSB.

One of the advantages of S-Tool is that 8-bit of images using a different approach where 8 bit of image file is produced by small size. This type of image have a palette of 256 RGB. In order to embed 8 bit of image by using S-Tool, S-Tool modifies the image by using 32 of palette from 256 RGB. The image that have a 32 of palette were duplicated 8 times to become total amount of 256. This method is implemented because storing 8 bits of data saving spaces due to its small size of the image.

There are a weakness where a secret information is hidden into 24 bits of image. Those who implement steganography method using S-Tool produces a large size of image. A large data is saving space is needed to save the image.

B. Hide and Seek

Hide and Seek version 4.1 is a free software tools that run on Disk Operating System (DOS). This tool only support image which GIF fail format. Besides that LSB is using to implemented watermark on GIF fail format.

The manual use of Hide and Seek software is same as S-Tool software, but the difference is Hide and Seek use 128 palette of RGB instead of 256 palette of RGB. Next, Hide and Seek works in 8-bits color coding only.

Basically, Hide and Seek contain two type of function, where one is for hidden data into GIF fail format, and one is for decrypt data. Both function are using command prompt to run the program.

One of the advantage of Hide and Seek is the image that had been steganography is small in size, hence the data saving space is enough to storing image.

The weakness of Hide and Seek is that all the program have to be run at command prompt. There are not provide Graphical User Interface for user. Hence, users may difficult to use this tool instead of other softwares that have provide Graphical User Interface. Besides that, Hide and Seek only works in 8 bits image only.

C. J-Steg

J-Steg software supported only JPEG fail format. J-Stego hides information into JPEG fail format. This is because JPEG fail format lossier compare to other image fail format. J-Stego using lossy compression algorithm to implemented hidden secret information into cover medium. JPEG is used in Internet widely because it is compressed and JPEG took small size of byte to store.

J-Steg using DCT (Discrete Cosine Transformation) technique in which data that has been compressed and stored as an integer data. DCT is required in this process where the data that have been stored converted into compression ratio.

The advantage of J-Steg is the image have been steganography was converted to compression ratio or in order word, the image was in smaller size. As result, the data space can be reduce and save space.

The weakness for J-Stego is when the compression that has been converted was loss or been alter, then the message that are hidden into the cover medium will be affected. Basically, secret information was hidden into image but for J-Tool, the secret message was hidden into compression coefficients.

Table 1 show the comparison of existing software and i-Mark in term of database, watermarking, algorithm, supported format and language.

Table 1: Comparison between existing software and i-Mark.

Details	S-Tool	Hide & Seek	J-Stego	i-Mark
Database	No	No	No	MySQL
Type of Watermark	Invisible	Invisible	Invisible	Visible and Invisible
Algorithm	LSB	LSB	DCT coefficients	Alpha channel (LSB)
Image Fail Format	GIF, Wav and others	GIF	JPEG	JPEG
Language	C	C	C	PHP and Java Script

In term of database, S-Tool, Hide and Seek, and J-stego did no using any database for storing data. The image that have been watermark was stored in user personal computer. While, i-Mark has it own database where image that had been watermark was stored into MySQL

On the other hand, S-Tool, Hide and Seek, and J-stego only have invisible watermark. While, i-Mark has two types of watermarking, which are visible and invisible.

i-Mark, S-Tool and Hide and Seek use LSB as the technique to apply steganography. While, J-stego use DCT coefficients.

Transmitting medium for J-stego and i-Mark is JPEG type file. JPEG was chosen because it is the most popular file format nowadays in communication and Internet. S-Tool support file format such as GIF, .wav and others. While Hide and Seek support GIF file format.

The Programming language for S-Tool, Hide and Seek, and J-stego are C language. While i-Mark use PHP and JavaScript as the programming language.

3. METHODOLOGY

Methodology that used to develop this i-Mark is Evolutionary Prototyping Methodology. Evolutionary Prototyping Methodology has four phases, which are planning, analysis, design and implementation.

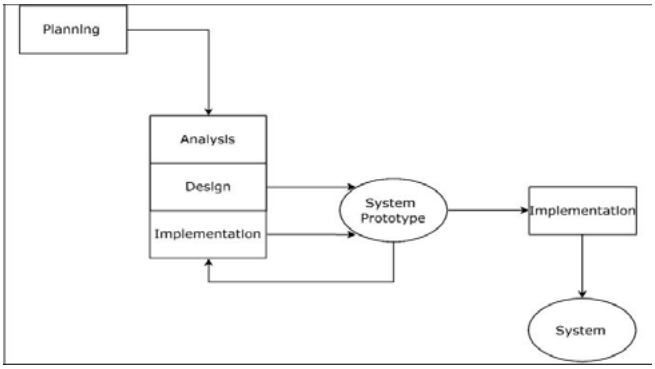

Figure 3: Evolutionary Prototyping Methodology [3]

A. Planning Phase

In planning phase, i-Mark is clearing describe by determined the objective and scope of developing i-Mark. Functionaries of i-Mark such as able to invisible and visible watermark an image is decide through the determination of objective and scope.

Gathering information was conducted to know the requirements by searching, accessing, observation and testing some watermarking system which are available online. Besides that, testing on some available online watermark are important to obtain some information on how to watermark an image is done. Meanwhile, accessing and observation of watermarking system is useful to gain the design interface for i-Mark.

Besides that, requirement gathering have also been carried out by studying and comparing a few similar watermarking system. Few similar watermarking system were observed based on functionalities. Observed similar watermarking system were conducted based on functionalities were used to understand and determined modules needed for i-Mark.

B. Analysis Phase

In this phase, information gathered from planning phase such as techniques of steganography is interpreted and compared.

From the interpreted and compared techniques of steganography, LSB technique was chosen to implement to i-Mark. Next, a further analyze of LSB method was conducted for further information such as coding to apply invisible watermark on cover of an image.

Besides that, in this analysis phase also compare of existing system, S-Tool, Hide and Seek, and J-Stego. Comparison of existing system were analyze to get overview idea of requirements. Requirement such as system requirement that system able to allow user to choose visible or invisible watermark and store the watermarked image in i-Mark.

C. Design Phase

The module involved in this system is hiding, extraction, encryption and

decryption. The system is developed using PHP language. Graphic design for the system interface is designed using Adobe Photoshop CS5. In addition, logo of i-Mark was design and placed on the top on the prototype.

Figure 4 show the logo of i-Mark.

Figure 4: i-Mark's logo

In addition, the prototype specifications is determined by implementing user requirement into the prototype. However, the prototype is a sketch for the user before the full system is produced. After successfully come out a prototype, testing was done to ensure the ability of the system was tested and meets the user requirements.

If there is any problem in the testing phase, the errors will be repaired and retested until the design development phase is successful.

D. Implementation Phase

This final phase requires developers to improve and complete all deficiencies have been found in the prototype to ensure i-Mark completely produced. The developer must evaluate the overall system, whether achieved compliance with users and compatibility with a software.

4. ANALYSIS AND DESIGN

This part describes the approach of the design and analysis of application developed. Design and application analysis is very important to explain in more detail the work flow of the system that developed as well as to build the system in accordance with the requirements of the user.

A. Flow Chart

Figure 5 shows the core functionalities provided for account users which are login, register, visible watermark, invisible watermark and view invisible watermarked images. User must login with an existed account to proceed to invisible watermark image.

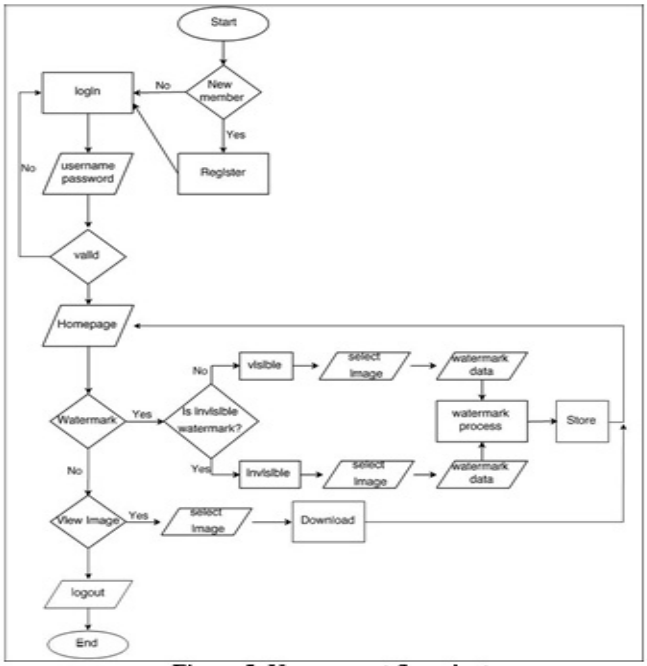

Figure 5: User account flow chart

B. Context Diagram

Context-level Data Flow Diagram clarify graphically the flow system. This diagram involved all the entities and data flows are then expanded so that the processes involved can be seen with more detail.

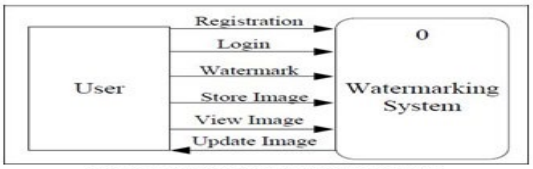

Figure 6: Context-level Data Flow Diagram

C. Data Flow Diagram Level 0

Figure 7 shows the data flow diagram level zero for the system. In the level 0 data flow diagram, there has five module namely registration, login, visible watermark image, invisible watermark image, and view invisible image. In registration module, user send a registration details and the data are store in a database name DATA_USER. Besides, login module is to verify the user that trying to enter into the system is member. Visible watermark image module is a module to watermark user image using text and download the watermarked image after the watermarking process is done. Invisible watermark image module is a module to implement steganography method to encode text into image. Invisible image would be stored into the database name IMAGE. View invisible image module is a module to enable user to view their own invisible image details such as invisible image, secret message and secret key.

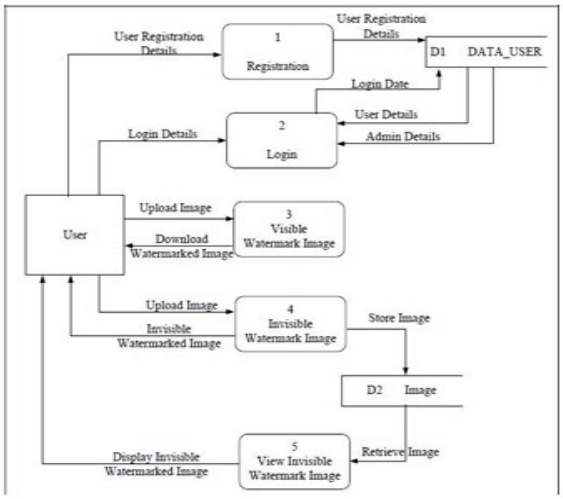

Figure 7: DFD level 0 for i-Mark

D. Entity Relationship Diagram

To describe the relationship between entities in i-Mark, a graphical model known as entity relationship diagram (ERD) was generated. There are two entities constituted to make the system functional. Each includes attributed which defines the content to be stored in database. Relationship is formed between entities to illustrate the dependency of each entity among each other.

Figure 8 shows the entity relationship diagram which demonstrates the relationships between entities in system

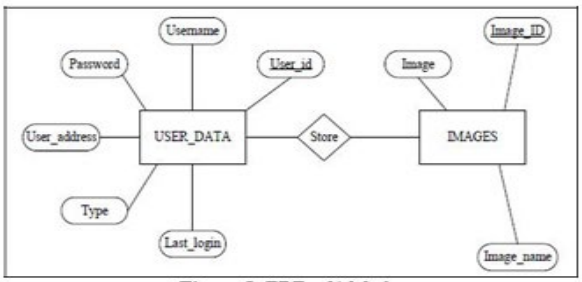

Figure 8: ERD of i-Mark

5. Implementation and Testing

In implementation phase, system design and analysis phase that defined in system specification would be used to come out a functional system. In system design, there are two important parts which are page interface and

database implementation. Page interface is a web pages that allow user to interact with the system. While, database implementation is used to enable user to create, delete or insert data into the system. Structure Query Language (SQL) was used in database implementation.

Testing phase was used to test the system operation. Testing phase was test to determine the level of system built achieved the system specification and user requirements. System functions test and user acceptance test were implement to test i-Mark system.

A. Register Module

Figure 9 show the new user register interface.

Figure 9. Register interface

B. Log in Module

Figure 10 show the log in interface for user to login into the system.

Figure 10: Log in interface

C. Visible Watermark Module

Before user can add text to an image, user must upload an image to be edited. Then user can add text into the image by click on the add text icon. User can edit the text by size, font, visibility level and color. Figure 11 show the edit text to an image interface.

Figure 11: Visible watermark interface

D. Invisible Watermark Module

In this module, user can choose to encrypt an image or to decrypt an image to obtain secret message that hidden in image.

I. Encryption

User must upload an image to able to do invisible watermark. After an image was uploaded, a box will be appear. User must enter a secret message and a secret key in the box provided. Figure 12 show the encryption interface.

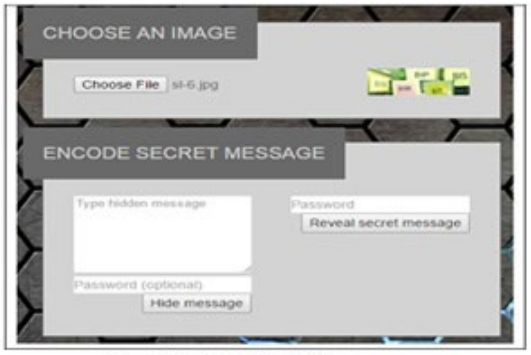

Figure 12: Encryption interface

II. Decryption

To do decryption, user must upload an image that contain secret message. If the image selected contain secret message, the secret message would be display for user after user enter the secret key to decrypt the image. While if the image did not contain any secret message, thus an alert message would be display for the user. Figure 13 show the decryption interface for user.

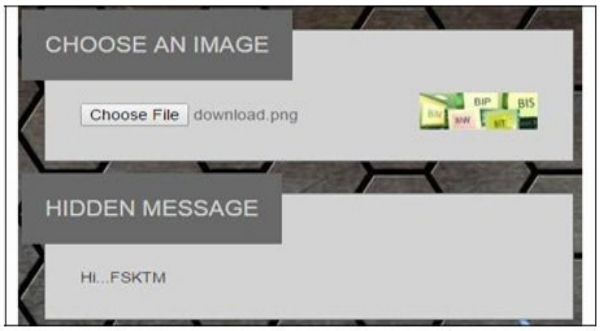

Figure 13: Decrypted interface

E. LSB Technique

Least significant bits in an image can be thought of as random noise and consequently does not result in human-perceptible difference as the amplitude of change is small.[4] Figure 14 show the some LSB algorithm that implement in this system.

```
// returns a 1 or 0 for the bit in 'location'
var getBit = function(number, location) {
   return ((number >> location) & 1);
};

// sets the bit in 'location' to 'bit' (either a 1 or 0)
var setBit = function(number, location, bit) {
   return (number & ~(1 << location)) | (bit << location);
};

// returns an array of 1s and 0s for a 2-byte number
var getBitsFromNumber = function(number) {
   var bits = [];
   for (var i = 0; i < 16; i++) {
      bits.push(getBit(number, i));
   }
   return bits;
};

// returns the next 2-byte number
var getNumberFromBits = function(bytes, history, hash) {
    var number = 0, pos = 0;
    while (pos < 16) {
        var loc = getNextLocation(history, hash, bytes.length);
        var bit = getBit(bytes[loc], 0);
        number = setBit(number, pos, bit);
        pos++;
    }
    return number;
};
```

```
// returns an array of 1s and 0s for the string 'message'
var getMessageBits = function(message) {
    var messageBits = [];
    for (var i = 0; i < message.length; i++) {
        var code = message.charCodeAt(i);
        messageBits = messageBits.concat(getBitsFromNumber(code));
    }
    return messageBits;
};
```

Figure 14: LSB Algorithm

F. Testing

User acceptance test were implemented to test i-Mark system. There are three part of testing, which are page interface design test, user interaction with system and system function test. Total of 30 participated to test the interface design and system function test. Figure 15 show the result of page interface design test. Overall, from the graph, navigation bar, text size, color and font, expectation of page and overall organization majority are satisfactory by user. Background color and clarity of message appear majority are marginally satisfactory by user. Figure 16 show the result of user interaction with the system. Overall from the graph, watermark images more quickly, and easy to operate majority are satisfactory by users. Access anytime and anywhere only marginally satisfactory by users and system is useful is very satisfactory by users. Figure 17 show the result of system function test. Overall, from the graph, login function, registration function, visible watermarking image, and display invisible watermarked image majority are satisfactory for user. Personal details display is marginally satisfactory by user and invisible watermarking image majority is very satisfactory for user.

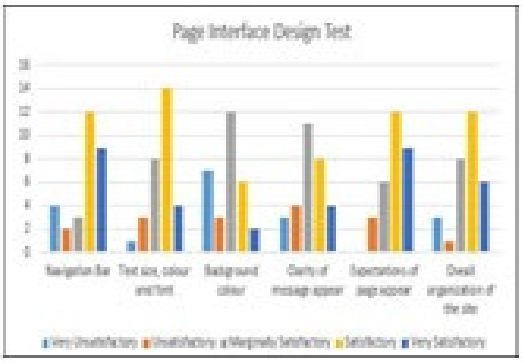

Figure 15: Page interface design test

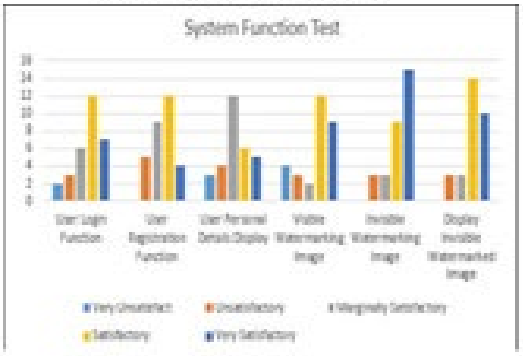

Figure 16: User interaction with system test

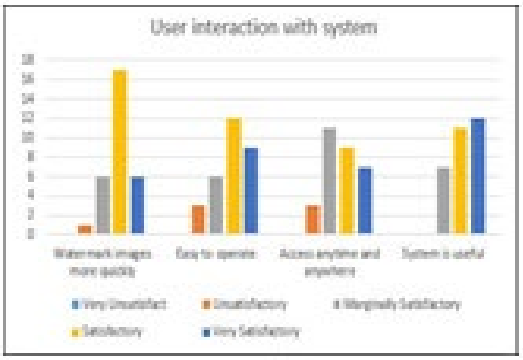

Figure 17: System function test

6. Conclusion and Suggestion

In conclusion, the system had been successfully developed and achieved objectives that were outlined besides fulfilling the system and users' requirements based on the current users' acceptance towards the system. However, there are still limitations of system that are yet to be discovered and improved in order to be able to cope up with the scalability of system in the future.

i-Mark aims to provide user a medium to watermark their image in web based. One of the advantages is protect the copyright of the user's image by steganography method. In addition, the application is web based which is easy to be used and applied by all user in anytime and any places with internet connection. Besides, additional features such as visible watermark which enable user to insert some text on the cover image for memories purpose, for example, location, time and description of the photo.

However, there are also limitation and disadvantages existed in the system. The limitation is i-Mark only limit to the image file type which is user only can watermark image file other than document file. Besides, i-Mark is not support for view by mobile platform. The system only can view by computer or laptop.

7. References

1. Alattar, A.M. (2004). Reversible watermark using the difference expansion of a generalized integer transform. IEEE. ISSN: 1057-7149. Pp. 1147-1156
2. Barni, M. , Piva, A. , Bartolini. F, & Cappellini, (1997). DCT-based Watermark Recovering without Resorting to the Uncorrupted Original Image. Image Processing, 1997. Proceedings, International Conference on Santa Barbara, CA. Print ISBN: 0-8186-8183-7. Pp. 520-523 vol. 1.
3. Dennis A. , Wixom B. H. & Tegarden D. Systems Analysis and Design: An Object-Oriented Approach with UML. John Wiley & Sons. 2015
4. Khazari, M., Sencar, H.T. & Memon, N. (2004). Image steganography: Concepts and practice.
5. Mohan Durvey and Devshri Satyarthi (2014). A Review on Digital Watermarking. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS). Volume 3, Issue 4, July-August 2014. ISSN 2278-6856.
6. Preeti Parashar and Rajeev Kumar Singh (2014). A Survey: Digital Image Watermarking Techniques. International Journal of Signal Processing, Image Processing and Pattern Recognition Vol. 7, No. 6 (2014), pp. 111-124