IMAGE STEGANOGRAPHY TO FACILITATE ONLINE STUDENTS ACCOUNT SYSTEM

Sara Manour Almutairi, Shaqra University, Shaqra, Saudi Arabia (sara.almutairi@su.edu.sa)
Adnan Gutub, Umm Al-Qura University, Makkah, Saudi Arabia (aagutub@uqu.edu.sa)
Maimoona Al-Ghamd, Umm Al-Qura University, Saudi Arabia (alghamdi.maimoona@gmail.com)

ABSTRACT

This work presents utilizing image based steganography for easy remembrance to access the online students account systems. The idea can be generalized to any university aiming to exploit the tool used for operative following-up from the school to its undergraduates and staff. The developed information technology tool will ensure efficient and active record review of the colleges and the academicians with less security breach problems from forgetting the passwords. The research modeled the online students' system involving image steganography to help hiding the passwords. The design is showing opportunity to reduce password resetting breach which can be serious problem affecting online records. The work is considered an opening direction for utilizing security techniques to help facilitate technology overhead problems.

Keywords: Key management, Online access, Image Steganography, Students records, Key remembrance.

INTRODUCTION

Computers have been in use for the last 60 to 70 years with most of its childhood to teenage life being only used in research facilities, or in organizations that dealt with massive mathematical data, renquiring high precision and fast processing. Fortunately things took a turn for the better when relatively minor companies and learning institutions realized how important this cutting edge technology could be in their day to day activities. This fact has led to computers being involved heavily in almost all places making it to the nowadays fact of internet of things and applications (Kendall, 2006).

This association of computers made-up the need for dedicated program platforms to run and organize our lives showing greatly positive impact (Milton, 2011). In fact, the rapid technological world had led to more people being interested in the computing industry and investing their time and resources encouraging computer and software engineers, information system analyst, programmers, computers designers, researchers and scientists to collaborate all together for developing computers to be focused in their applications. Fortunately, learning institutions all over the world are working so hard to fully modernize the learning process by incorporating technology more and more in the learning process (Ramakrishnan, 2003). This includes centralized management systems and online services that can be accessed from anywhere on the net.

Universities are always composed of various management processes like record keeping, content distribution, file management, content generation, communication and administration processes (Walczak, 1999). These processes may be governed by the kind of management structure that is used and it will always be almost the same process repeating over and over in each different units or department of the organization. Online student account where by students can dynamically access contents from the comfort of their places leads to an effective centralized management process as it leads to speedy storage and retrieval of contents by administration and the students (Walstrom, 2001). Early traditional methods were subject to time consuming, a lot of paper work, data loss and ineffective communication which modern technology is addressing

The online systems need authentication passwords from all users to allow them to access the records based on their specific privileges (Alassaf et al., 2018). These passwords are to be secured for intended members to keep as for authentication entree is needed. The challenge occurs since this system forces the users to remember hard secret passwords, especially when the systems require changing passwords frequently. This problem impact raise clearly as the individuals are requested to hold different number of passwords constructed specific for the application utilizations (Gutub & Alaseri, 2018). This paper study the online students' system from its functional point of view as well as fixing the password remembrance problem putting this secret hidden in a multimedia cover (stego-cover) based on user choice. This selection gives users responsibility to fully remember the intended stego-cover instead of the secret changing password, i.e. imagining it as memorizing means definitely simpler to recall every time wanted.

Steganography is a data hiding scheme that covers the knowledge of existence of the secret data. It is emerging the sensitive information within stego-cover media data that can be any electronic form of text, audio, pictures or video. Many steganography hiding techniques have been presented (Gutub, 2010), some relied on the spatial domain benefitting from popularity and simplicity in implanting and utilization (Gutub et al., 2008). Others base its idea on the transform domain to focus on robustness (Hussain et al., 2018). The image-steganography is found more popular making the dedication of this work exist studying the almost redundant Least significant bit (LSB) as stego-hiding locations (Alanizy et al., 2018). The exact number of LSB bits to be used for hiding varies as detailed by intended techniques used. For example, the pixel indicator techniques as proposed in (Gutub et al., 2008) pretend many layers, such as triple-A method that is built on random selections (Gutub et al., 2009) as well as RGB image-stego scheme looking at the intensity as its focused technique proposed by Parvez et al. (2008, 2011). This work also considers the truth table and determinate array-based techniques as possible pixel indicator stego schemes investigated (Abu-Marie et al., 2010). In fact, these stego-techniques considered within this research are interestingly fair to be compared. They are proven practical for hiding and recovering secrecy for the sensitive online account systems.

This study proposes hiding the secret password to access the registration page using many LSB image-steganography schemes hoping to increase the authentication security (Alsaidi et al., 2018). The research related few stego-methods comparing their hiding security and capacity factors. The paper flow can be outlined by first presenting an overview of online systems and its preliminaries as literature survey. Then, section three covers the online students account system showing the problem needing to involve steganography. Section four presents the stego-techniques tested in this study. Fifth section presents our idea of utilizing image steganography to be used as another option replacing normal text-password detailing the results and comparison remarks. Finally, the work is concluded in Section six summarizing the paper.

LITERATURE REVIEW

The current internet-of-things (IoT) society makes great demands on educational institutions to be very technologically advanced. Many societies depend on universities, to be leading, developing and innovating IoT technology (Milton, 2011). Unfortunately, educators believe that adapting technology may be the potential power to solve the societal change pressure in attitude and delivery of information in institutions (Walstrom, 2001). Accordingly, universities should be the principal in delivering and providing learning experiences that involve and agree with all requirements of the students, faculty and staff (Ramakrishnan, 2003). This is only possible by providing modern and reliable means of communication channel between themselves. Universities should try linking the real-world modern e-challenges (Walstrom, 2001), i.e. to involve information systems platform integration and to support data-intensive applications (Ramakrishnan, 2003). This technology role is considered massive for providing a richer and more exciting environment for communication (Kendall, 2006).

Online systems are giving students the opportunity to learn how to showcase their accomplishments of trustworthy work to intended audience using non-traditional media options, accommodating individual differences between themselves as students and the staff. Generally, information systems are used for decision making, planning, organizing, staffing, directing and controlling. Kendal (2006), define database management system (DBMS) as the e-platform for organizing the info-storage and retrieval capabilities, and all data storing issues within the database systems. In fact, Kendall (2006) also defines system development life cycle (SDLC) specified for design and analysis as it holds the systems practice records using specific cycle of analysis and user actions. The information requirements of an organization constantly change as the organizations grow, matures and reacts to internal and external forces. Normally, a computer-based information system goes through SDLC as planned tactic used in organizations to run information system properly via following "six phases: preliminary investigation, system analysis, system design, system development, and system implementation and evaluation, and system operation and maintenance" (Kendal, 2006), as defined below:

- **Preliminary investigation** considers feasibility investigation figuring real justifications to build the system. It links the possibilities to reasonable pricing, then assist to give decision to go ahead with specifications and their costs.
- **System analysis** considers the system's facilities, restraints, and objectives, which should be recognized step-by-step with end customers. This step is intended to refine the system specifications.
- **System design** involves partitions requirements and its effect in overall system architecture.

- **System development** considers the actual code writing of the program. It should be revised verifying that each part meets the exact specifications. The Output is the program units that make the system.
- **System implementation and evaluation** looks for integration of separate program components. The units are then tested via step-by-step collaboration manner.
- **System operation and maintenance** should be then taking place. It should be allowing amending errors that were not found before refining or trying the system. Especially in quick adjustments needs, it is recommended to work it out immediately, hence resulting to an always improved enhanced system.

ONLINE STUDENTS ACCOUNT SYSTEM

The online students account system research involves data requirement, data collection techniques, data analysis used and a brief description of the activities affected. To fulfill the online architecture meeting the requirements, system analysis had done investigation on needed information on inputs, process, outputs, timings and controls required. The students' population, target population for this research, can be any members of the university. The methods used for the research includes use of tools like observations, interviews, and questionnaire. However, focus groups, online discussions chats and online forums were proposed for online data collection. The research used interviews, questionnaires, secondary sources and observations to collect the necessary data, as needed for the pilot study research. The interviews have been done as face to face discussion as part of the sample that would be chosen from the study population. Questioners was beneficial allowing freedom un-influenced opinions answering a list of questions with multiple answers, which was given to different groups of the sample selected from the study population. Secondary sources have been collected from literature reviews, outranked sources and the internet giving some indication of the system out-of-box view.

The research statistical methods analyzed the sample results from the data collected and the tools have been organized accordingly. The tools selected to develop the system have been: PHP, HTML, CSS, JavaScript, MySQL, WAMPSERVER, and MOZZILAFIREFOX.

- PHP, Pre-Hyper Text Preprocessor: giving the system interactivity when it is online.
- HTML, Hyper Text Mark-up Language: developing system layout.
- CSS, Cascading Style Sheets: making the system layout be attractive for flexible appearance.
- JAVASCRIPT: for animations in the system.
- MYSQL, Structured Query Language: for coding the database.
- WAMPSERVER: for hosting system testing and creating the needed driving database.
- MOZZILA FIREFOX: building the browser platform used to launch the system.

The system beginning Interfaces can be shown as Figure 1 representing the main home page of the student online system, Figure 2 showing the traditional login via text username and password, and Figure 3 is the system registration form to be completed once at the beginning of using the online platform. Note that this traditional system accepts the password as text only (Figure 2), as the online systems need authentication passwords from all users as permission strategy to see/modify the records formed obeying definite rights. These passwords are normally to be preserved secure by anticipated participants as required, i.e. for authentication access. The challenge here comes from the users' remembrance possibility especially as the individuals need more number of passwords to recall according to the usage real life applications (Gutub & Alaseri, 2018). This study challenge focus on clear online students' system password remembrance problem, putting this secret to be hidden adopting image steganography assuming it to be easier for the user as detailed in section.

IMAGE STEGANOGRAPHY METHODS

Several suitable image steganography techniques are found in the literature, however, not all are easy to be utilized and tested. To proof the concept, we selected several simple image-based least significant bit (LSB) schemes to test storing the password, similar in principle to the work reported at (Gutub & Al-Ghamdi, 2019a). The work experimented five similar least significant bit (LSB) steganography schemes pretending to get fair comparisons. The research studied the security and capacity as known standard judging remarks to link passwords-remembrance to hiding within image steganography, pretending starting this research field out of the box direction. We have used the following five stego methods, for comparison and analysis, as listed below:

- Vibrant color image steganography (Parvez & Gutub, 2008)

- Pixel Indicator Technique (Gutub, 2010)
- Pixel Indicator High Capacity Tech. (Gutub et al., 2008)
- Triple A Steganography (Gutub et al., 2009)
- Truth Table Steganography (Abu-Marie et al., 2010)

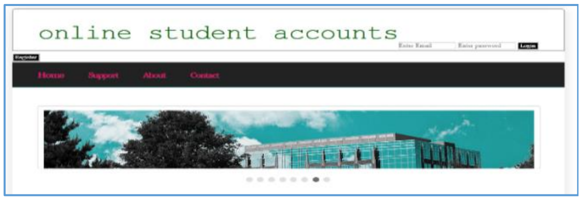
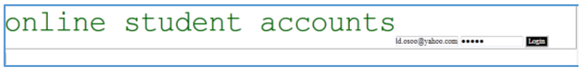
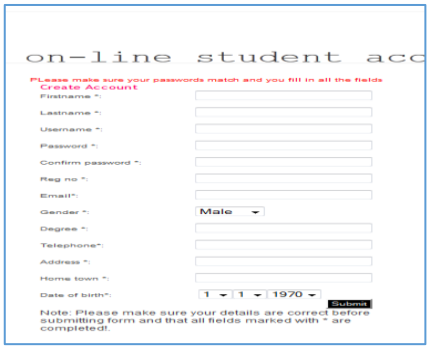


Fig. 1. Home page



ld.osoo@yahoo.com •••••

Fig. 2. Student traditional Login



PLease make sure your passwords match and you fill in all the fields

Firstname *:
Lastname *:
Username *:
Password *:
Confirm password *:
Reg no *:
Email*:
Gender *: Male
Degree *:
Telephone*:
Address *:
Home town *:
Date of birth*: 1 1 1970

Note: Please make sure your details are correct before submitting form and that all fields marked with * are completed!.

Fig. 3. Registration page

AUTHENTICATION VIA STEGANOGRAPHY INVOLVEMENT

This work is proposing to involve image steganography to help as another option instead of text-password. The idea gives the user within the registration page (Figure 3) to select an image as password stego-holder. This selected stego-cover is called whenever needed as alternative key to the password chosen, imagining to be used as storage means used every time considered necessary. The interface of this proposed stego-online access can be simplified as shown in Figure 4.

Employing image steganography, to recall passwords, i.e. to access the students account system, projected storing the text-password in any picture (or image) based on users' preference, like the previous research serving counting-based secret sharing presented in (Gutub & Al-Ghamdi, 2019) and hash functions of (Almazrooie et al., 2018). This work is further useful for protecting medical records against cybercrimes within Hajj period by 3-layer security as discussed in (Samkari & Gutub, 2019) but needs further focus research study. The investigation of steganography selection suitable to implemented assumed a traditional image as stego-cover for experimentation. The research assessed all five stego-methods corresponding to the key known parameters to determine its practical usefulness for hiding secret password, i.e. security and capacity. The security have been tested via histogram of the R, G and B channels comparing them before hiding data and after the hiding to sense the amount of visible distortion in unified manner. The study evaluated the capacity by considering the amount of bit per pixel to be hidden assuming the different methods. To be consistent with previous work reported at (Gutub & Al-Ghamdi, 2019a), the research showed its results assuming stego-cover standard picture of a known palace named Alhambra (68160 pixel), as can be observed in Figure 5.

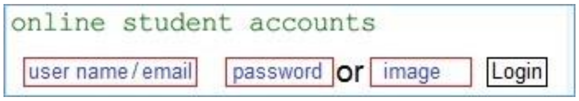


Fig. 4. Proposed access authentication allowing image steganography.

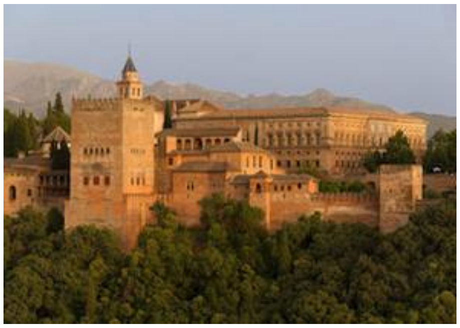


Fig. 5. Alhambra image (320x213)

A. Security

The research investigated all five LSB stego-schemes simulated hiding the password within the stego-cover: Alhambra, used for testing its histogram before and after hiding. Interestingly, it did not show visual deference indicating that all image steganography techniques adopted are acceptable, i.e. showing no variation, as an example shown in Figure 6.

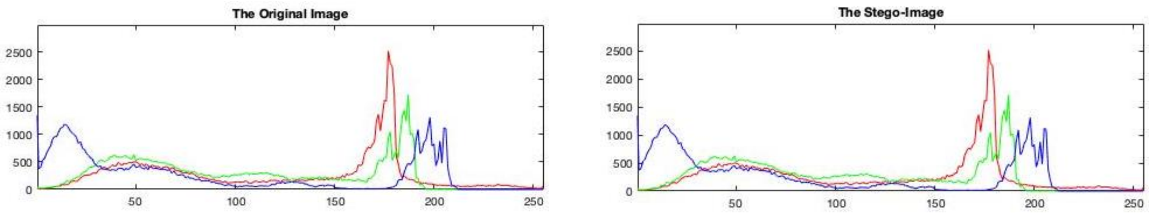


Fig. 6. Histogram assessment of applying LSB steganography for security study purposes

B. Capacity

The capacity of hiding bits within images need to be investigated making sure of its sufficiency and can be used as preference measure to choose appropriate stego-technique. All five steganography methods have been compared hiding the same secret password data utilizing all stego-methods following the security investigation remarked in (Gutub et al., 2011) and benefitting from previous work presented in (Khan & Gutub, 2007; Gutub & Fattani, 2007; Gutub et al., 2010). The experimentations, as listed in Table 1, showed variations of stego-schemes using methods clearly affecting the bit per pixel (bpp) calculation. It gives the intended ambiguity proofing the required unpredictability within hiding different than security studies in (Gutub et al., 2011; Gutub & Fattani, 2007; Almazrooie et al., 2018). In fact, we noted within the results that the capacity changed positively with the triple-A scheme as well as the vibrant color stego-method. Unlike the truth table steganography scheme of worse capacity making it the unrecommended choice, which is providing some flexibility preference selection to be given to the security executive to use. This can be used as factors of selection considering more parameters to be investigated to complete this study.

TABLE 1 CAPACITY INVESTIGATIONS

Study steganography image: Alhambra	**bpp capacity remarks**	
Pixel Indicator High Capacity Tech.	13	11%
Triple A Steganography	7.30	13.68%
Truth Table Steganography	16.8	5.94%
Vibrant color image steganography	4.5	22.06%
Pixel Indicator Technique	11.9	8.3%

CONCLUSIONS

Through the research, we have addressed the online student system authentication practicality utilization benefitting from different security LSB steganography methods. The work focussed on password practical remembrance issues which found to be improving as steganography is involved, i.e. to hide the open presence of the secret personal passwords. This steganography engagement forced the fraud or interfering of the online student account approach access secure as intended.

The study investigated to improve the practical usability of the student online system by enhancing the memorization possibility via integration to image steganography schemes. Image steganography is adopted appropriate for keeping key passwords and permitting the entry to assist users giving the flexibility of image selection based on personal choice. The research verified the upgraded student online system via five unique LSB image steganography methods. The stego-approaches are chosen to be similar based on LSB stego main idea showing acceptable execution and implementation theme. The measured investigated image-stego techniques have been comprising, pixel indicator high capacity tech, triple-A steganography, truth table steganography, vibrant color image steganography, and pixel indicator technique. All five image steganography methods have been evaluated considering their histogram deformation overview security as well as bit per pixel (bpp) image storage capacity. The work concluded that the truth table steganography method and the triple-A image stego-scheme both achieved acceptable security performance. This security remark can be also valid for the pixel indicator technique but with it achieving interesting bpp capacity making it the satisfactory choice less than the vibrant colour image steganography, i.e. showing highest capacity.

The work is still considered in its early stage. We are currently planning to test dissimilar other steganography techniques openly, i.e. stego methods based on transform domain as well as spatial domain. Furthermore, the study can advise to explore merging other security authentication schemes such as hashing, cryptography, or watermarking, which may be interesting for the evolving security needs. The work can also consider blockchain applications, i.e. for achieving remembrance features and more security of online systems as well as cloud computing.

ACKNOWLEDGMENT

Thanks to the wonderful scientific cooperation between researchers from the two institutions, Computer and Information Technology College at Shaqra University, and Department of Computer Engineering within College of Computers and Information Systems at Umm Al-Qura University, Makkah; all supported by Ministry of Education under the government of Saudi Arabia.

REFERENCES

Abu-Marie, W. Gutub, A. and Abu-Mansour, H. (2010). Image Based Steganography Using Truth Table Based and Determinate Array on RGB Indicator. *International Journal of Signal and Image Processing*, 1.

Alanizy, N., Alanizy, A., Baghoza, N., Al-Ghamdi, M. and Gutub, A. (2018). 3-Layer PC Text Security via Combining Compression, AES Cryptography, and 2LSB Image Steganography. *Journal of Research in Engineering and Applied Sciences (JREAS)*, 3(4), 118-124.

Alassaf, N., Gutub, A, Parah, S. and Al-Ghamdi, M. (2018). Enhancing Speed of SIMON: A Light-Weight-Cryptographic Algorithm for IoT Applications. *Multimedia Tools and Applications: An International Journal*, ISSN 1380-7501.

Almazrooie, M., Samsudin, A., Gutub, A., Salleh, M.S., Omar, M.A. and Hassan, S.A. (2018). Integrity verification for digital Holy Quran verses using cryptographic hash function and compression, *Journal of King Saud University - Computer and Information Sciences*.

Alsaidi, A., Al-lehaibi, K., Alzahrani, H., AlGhamdi, M. and Gutub, A. (2018). Compression Multi-Level Crypto Stego Security of Texts Utilizing Colored Email Forwarding. *Journal of Computer Science & Computational Mathematics (JCSCM)*, 8(3), 33-42, DOI: 10.20967/jcscm.2018.03.002.

Gutub, A. and Fattani, M. (2007). A Novel Arabic Text Steganography Method Using Letter Points and Extensions, *WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE)*, Vienna, Austria.

Gutub, A., Ankeer, M., Abu-Ghalioun, M., Shaheen, A. and Alvi, A. (2008). Pixel Indicator High Capacity Technique for RGB Image Based Steganography. *WOSPA 2008 –5th IEEE International Workshop on Signal Processing and Its Applications*, University of Sharjah, U.A.E.

Gutub, A., Al-Qahtani, A. and Tabakh, A. (2009). Triple-A: Secure RGB image steganography based on randomization. *IEEE/ACS International Conference on Computer Systems and Applications*, Rabat.

Gutub, A. (2010). Pixel Indicator Technique for RGB Image Steganography. *Journal of Emerging Technologies in Web Intelligence*, 2(1).

Gutub, A., Al-Alwani, W. and Bin-Mahfoodh, A. (2010). Improved Method of Arabic Text Steganography Using the Extension 'Kashida' Character. *Bahria University Journal of Information & Communication Technology (BUJICT)*, 3(1), 68-72.

Gutub, A., El-Shafei, A.R. and Aabed, A. (2011). Implementation of A Pipelined Modular Multiplier Architecture for GF(P) Elliptic Curve Cryptography Computation. *Kuwait Journal of Science and Engineering*, 38(2B), 125-153.

Gutub, A. and Alaseri, K. (2019). Hiding Shares of Counting-Based Secret Sharing via Arabic Text Steganography for Personal Usage, *Arabian Journal for Science and Engineering*.

Gutub, A. and Al-Ghamdi, M. (2019). Image Based Steganography to Facilitate Improving Counting-Based Secret Sharing. *3D Research* - Springer, ISSN 2092-6731, 10(1).

Gutub, A. and Al-Ghamdi, M. (2019a). Accommodating Secret Sharing Technique for Personal Remembrance via Steganography. *IEEE International Conference on Fourth Industrial Revolution (ICFIR),* DOI: 10.1109/ICFIR.2019.8894784, Manama, Bahrain.

Hussain, M., Wahab, A.W.A., Idris, Y.I.B., Ho, A.T.S. and Jung, K.H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, 65, 46-66.

Kendall, K. and Kendall, J. (2006). *System Analysis and Design*. Prentise-Hall., New jersey.

Khan, F. and Gutub, A. (2007). Message Concealment Techniques Using Image Based Steganography. *4th IEEE GCC Conference and Exhibition*, Manamah, Bahrain.

Milton, S. (2011). Ontological comparison and Evaluation of Data modelling frameworks, *PhD Thesis*. University of Melbourne.

Parvez, M.T. and Gutub, A. (2008). RGB Intensity Based Variable-Bits Image Steganography. *APSCC 2008 – 3rd IEEE Asia-Pacific Services Computing Conference*, Yilan, Taiwan.

Parvez, M.T. and Gutub, A. (2011). Vibrant Color Image Steganography using Channel Differences and Secret Data Distribution. *Kuwait Journal of Science and Engineering (KJSE)*, 38(1B), 127-142.

Ramakrishnan. R. (2003). *Database management systems*. McGraw.

Samkari, H. and Gutub, A. (2019). Protecting Medical Records against Cybercrimes within Hajj Period by 3-layer Security. *Recent Trends in Information Technology and Its Application*, 2(3),1–21, DOI: 10.5281/zenodo.3543455.

Walczak. S. (1999). A Re-evaluation of information systems publications forums. *Journal of Computer Information Systems*, 40(1), 88-97.

Walstrom. K. (2001). Forums of information system scholars. *Information and Management*, 39(2), 117-124.