Journal of Engg. Research Vol. 11 No 3 pp.100-111 **DOI:10.36909/jer.13761**

Engineering Graphical Captcha and AES Crypto Hash Functions for Secure Online Authentication

Nafisah Kheshaifaty and Adnan Gutub*

Computer Engineering Department, Umm Al-Qura University, Makkah, Saudi Arabia

** Corresponding Author Email: aagutub@uqu.edu.sa*

Submitted **:** 01-04-2021

Revised **:** 06-07-2021

Accepted **:** 20-09-2021

ABSTRACT

Password alone is currently not trusted for user online authentication and security as threats from hackers continue to grow, requiring highly efficient defense safeguard protection against unauthorized users. Therefore, CAPTCHA techniques came into the picture as an automated assistance to distinguish between humans and robots. The CAPTCHA has several applications in the online security domain requiring to be merged with encrypted hash function benefitting from the facility of the graphical password schemes. This paper proposes engineering an authentication technique using graphical CAPTCHA with an AES encrypted hash password to maintain applicable security accessing systems. We propose three layered security system that joins highly efficient security mechanisms to avoid users' stress of entering password many times or different other hectic routines in order to save account accessing.

Keywords: Access Control; Authentication; Captcha; Cryptography; Encryption; Hashing.

INTRODUCTION

The user authentication of online systems plays an important role in the protection of the personal sensitive information from unauthorized hackers (Alanizy et al., 2018). It also prevents systems from losing the classified data which is becoming essential for block-chain applications (Altalhi & Gutub, 2021). Nowadays, the normal technique used for authentication is via secure passwords becoming vulnerable to denial of service attacks as well as password guessing techniques (Al-Shaarani et al., 2020). To mitigate these user authentication attacks, researchers propose involving a *Completely Automated Public Turing tests to tell Computers and Humans Apart* (CAPTCHA) approach, that prevents computer generated program to access the system (Kheshaifaty & Gutub, 2020). There are three types of CAPTCHA common easy tools used, based on image, sound, and text schemes. Interestingly, text-based CAPTCHA is the most widely used scheme (Kolekar & Vaidya, 2015), considering text language community practicality (Gutub et al., 2010), as shown in Figure 1.

Figure 1. Graphical text CAPTCHA

This engineering research proposes utilizing Password Guessing Resistant Protocol (PGRP) to control the online password predicting attacks and the brute force attacks (Ahmed et al., 2016). The method is barring sign-in attempts from undesirable web servers similar in principle to trusting counting-based secret sharing (Gutub et al., 2019) which is advanced for proper authentication via M-Blocks partitioning (Gutub & Al-Qurashi, 2020). The PGRP includes two interfaces, namely graphical-user interface (GUI) and character-based interface, which is found common for most IoT technologies (Shambour & Gutub, 2022). This work adopted the estimation attack against ten popular real-world captcha schemes provided by google.com pretending to break them. Our study further compared the security, investigating the attacks with two common methods of eight captcha (solving services) and nine online image recognition services. The results of analysis proposed our 3-layer scheme to combine captcha with hash and encryption following the published 2-level stego-crypto security combination (Alkhudaydi & Gutub, 2021). Our proposal is based on the distance, the process of zooming, transverse displacements, and twisting characters, which all can be closely linked to capture Captcha image styles.

LITERATURE REVIEW

As part of the literature review, different methodologies based on secure access were analyzed in order to determine loopholes to be addressed. For example, Vaithyasubramanian (2016) notes that audio CAPTCHA used to prevent auto brute force attempts that can be helpful for visually impaired people. Audio security is helpful in current applications as other multimedia get corrupted or less useful (Al-Juaid & Gutub, 2019). This research audio CAPTCHA suffered noise of speakers, which matched the background noise, and found having finite set of vocabulary reducing its security. Other CAPTCHA schemes used puzzle-based manipulation, which involved puzzles, such as Cascading style sheet, JQuery, and HTML (Ali & Karim, 2014) or any complex image-based authentication (Al-Roithy & Gutub, 2021). The puzzle-based CAPTCHA showed authentication testing, but requested puzzle-based widget to provide support for installing web information. Therefore, Cui et al. (2010) used CAPTCHA to prevent malicious advertisement attacks on the web by multi-layer CAPTCHA techniques. Their work bonded vision theory to be easy for human identification in an optimization structure. Statistical function variance was employed for the mitigation of the attacks in a complex manner, as found appropriate for complex applications such as medical and airline services (Alsaidi et al., 2019).

Since CAPTCHA can be categorized on OCR relation, Kaur (2016) proposed non-OCR Math CAPTCHA based on Boolean algebra. This authentication technique showed good attack control rate, but was also found aligned to a complex database that cannot be generalized to many other applications. Similarly, Althamary and El-Afy (2017) proposed accessing methodology based on passkey with a combination of user password and the characters of CAPTCHA. Although, the results of this technique show remarkable gain by resolving attack issues of key logger, phishing, and password guessing, it is unfavored because of its limitation on the agreement with the user.

Kulkarni and Malwatkar (2015) presented graphical CAPTCHA method that utilizes image processing along with AI techniques. The research provided multiple image challenges to mitigate the shoulder surfing security issue, as found very suitable for desktop application security. However, the drawback of this scheme is in utilizing space for multiple passwords involved by the user running every login session. Lv et al. (2016) notes that English language-based CAPTCHA is easy to understand compared to Chinese CAPTCHA that is more complex to solve. The distortion and noise have been resolved by involving conventional neural network (CNN) approaches resulting in accuracy improvement, but with complex designing. Furthermore, Zhang et al. (2017) argues linking to segmentation to improve CAPTCHA recognition. Their work coded vertical projection to the segmentation of the characters, but found reduction in its security reliability.

Tirthani and Ganesan (2014) proposed user authentication based on sharing unusual keys to prevent DOS attacks. The session of key generation is done through Diffie-Hellman key exchange scheme. Similarly, Alta vista website adopted a private captcha system to differentiate between computer and humans. Relatively, Malutan and Grosan (2015) introduced two new schemes of graphical passwords abbreviated as COSS and CODP schemes, which reduce the chances of shoulder surfing attacks. This method shows strangest entropy bit as compared to other schemes since it generates strong passwords by using set of questions and answers.

Table 1 summarizes the performance of recent related researches considered most relevant to the evaluation of our study. The table assigned notations to be used within this paper for precise symbolization, i.e. throughout the work. The brief comparison links the cost, productivity, user satisfaction, and security quality to further justify the need for our 3-layer authentication research.

Table 1. Performances of relevant researches showing its notation for using within this study.

Study	**Research Paper Notation**	**Performance Evaluation Criteria**			
		Cost	**Productive**	**Customer Satisfaction**	**Quality**
(Vaithyasubramanian, 2016)	V-2016	High	Good	Yes	OK
(Ali & Karim, 2014)	A-2014	Moderate	Good	Yes	OK
(Cui et al., 2010)	C-2010	High	OK	No	Poor
(Kaur, 2016)	K-2016	High	Good	Yes	OK
(Lv et al., 2016)	L-2016	Moderate	Low	No	Poor
(Zhang et al., 2017)	Z-2017	Moderate	Low	No	Poor
(Ahn et al., 2003)	A-2003	Moderate	Low	No	Very poor
(Tirthani & Ganesan, 2014)	T-2014	Moderate	Low	No	Poor
(Chen et al., 2014)	C-2014	High	Good	Yes	High
(Liao et al., 2005)	L-2005	Moderate	Ok	Yes	Ok
(Juang et al., 2008)	J-2008	Low	Good	Yes	High
(Das et al., 2007)	D-2007	Moderate	Ok	No	Poor
(McLoone & McCanny, 2003)	M-2003	Moderate	Ok	Yes	Ok
(Merler & Jacob, 2009)	M-2009	Moderate	Good	Yes	High
(Gossweiler et al., 2009)	G-2009	High	Ok	No	Ok
(Zhang et al., 2019)	Z-2019	High	Good	Yes	High

The study showed that most of current applicable researches utilized two-layer authentication (Al-Ghamdi et al., 2019.), and some unacceptable single authentication (Al-Nofaie & Gutub 2020), were all considered to be vulnerable in today's advancing IoT and AI technology (Alassaf & Gutub, 2019.). Therefore, our proposal targeted 3-layered authentication research to provide practical accessing trustful security.

In this paper, the engineering methodology measured directional based graphical password technique to be used to modify pass faces scheme with direction image. Shoulder surfing proof authentication has been shown because the user would not click on their picture directly in this process. Since the hashed value is immutable, the algorithm of probability is used. This algorithm keeps the right, left, top and bottom values of the photos that have been clicked. According to their directions the image will be combined and all values are compared with the database value of the hashed value. This method is helpful in securing authentication process. We, in this paper, used human computation method to gain click points or Pass Points from the user and to predict hot spots.

PROPOSED APPROACH

Graphical text CAPTCHA is commonly used for the authentication of humans from bots (Kheshaifaty & Gutub, 2020). Its drawback can be in usability as humans may find difficulty reading them due to high distortion to be secure. This paper proposed the engineering methodology integration of graphical CAPTCHA with encryption standard (AES) 256 bits and SHA 256 hash function to overcome these usability security challenges (Kaur, 2016). This engineering methodology improved the security for the system and user data from unauthorized attempts improving research in (Kahri et al., 2013). Figure 2 shows the proposed system CAPTCHA Hash Encryption framework.

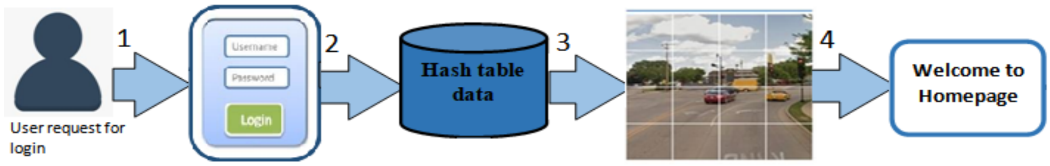

Figure 2. Proposed system framework

The research proposed graphical password to prevent active guessing attacks and shoulder surfing attacks as well as bot auto programs and replay attacks, justifying common CAPTCHA technology built on graphical password, known as (CaRP) (Kulkarni & Malwatkar, 2015). CaRP provided reasonable usability and security (Kahri et al., 2013), as our login part is designed to start the system by providing a new image every refresh or new attempt. To access the system the user has to click on the same point based on visual CAPTCHA creation of CaRP images. Figure 3 show cases a sample of the CaRP images introduced in our system.

Figure 3. Example of CaRP images used in our proposed system

The second part building our proposed engineering system adopted the Standard AES (256) bits encryption, as a block cipher compulsory technique for maintaining security (Alsaidi et al., 2018). The original data is scrambled by mathematical calculations. The encrypted data is to be shown in the original form only with the help of the key (Shimazaki et al., 2016). AES is working with a symmetric key cipher. For encryption and decryption purposes the same key is used. This symmetrical algorithm needs less computational power and faster to run. AES 256 bits provide security through a complex level of encryption. Figure 4 shows the AES overview mechanism.

The third component of our proposed engineering mechanism consists of hashing. In hashing, the resolution of collision can be resolved by utilizing specific function and hash lookup tables (Shimazaki et al., 2016), as it greatly affects the complete system performance. Figure 5 highlights the mechanism of the hash table.

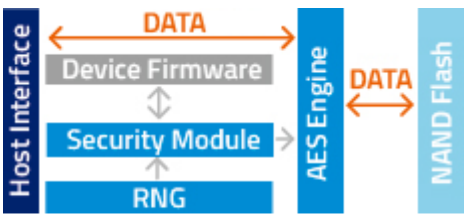

Figure 4. Secure mechanism of the AES 256

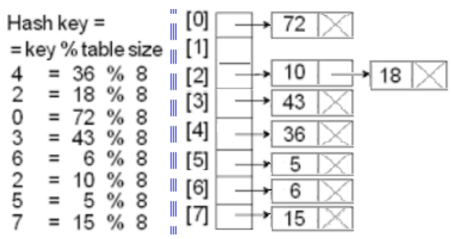

Figure 5. Hash table performance

The applications of hash functions are popular to be considered in the hash table structure found appropriate utilizing SHA 256, as secure functions improving SHA-1 (Zhang et al., 2019). Table 2 briefs the SHA specs. Beside SHA 256 security and speed strength, it is found compatible with encryption function AES 256 bits, making our selection appropriately tuned. The implementation of the system is run on JAVA platform as generated by the multiple blocks of 512 each bit. The cycles of our SHA 256 take the input expanded in words of 32 each bit similar to work of (Kahri et al., 2013). Figure 6 shows a type of iteration.

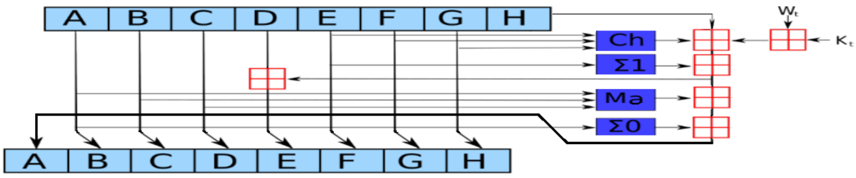

Figure 6. An iteration of SHA-256 hash function

Table 2. Hash function Specification

SHA 256 Hash Function				
Function	**Digest size**	**Collision**	**First preimage**	**Throughput (MiB/second)**
SHA256	25	2^{128}	2^{256}	275

The proposed engineering scheme consists of 3 layers of graphical CAPTCHA, AES 256 bits along with SHA 256 hash function, as secure practical mechanism for online website services similar in objective to the work in (Samkari & Gutub, 2019). If the bots programs breaches the security of the any single layer, then it would be complex to break the security of the other 2 layers.

Table 3 shows how the proposed system has attractive performance in terms of security and usability defending security risks of password guessing, keylogging, phishing, and unauthorized user access to the system, linking the references with proper study used notations.

Table 3. Hash running assessment of proposed vs. other relative techniques

Technique	Notation	Speed	Performance	Size
Graphical Passwords Captcha - Primitive Based on Hard AI (Liao et al., 2005)	L-2005	N/A	N/A	N/A
Secure Scheme for CAPTCHA-Based Cloud Authentication (Cui et al., 2010)	C-2010	N/A	N/A	N/A
Improved DROP security: hard AI cloud (Merler & Jacob, 2009)	M-2009	N/A	N/A	N/A
Password- based identity authentication system (Chen et al., 2014)	C-2014	881.7 ms	7.6% << SHA1	32 chars hash
Online password sensor-based authentication (Zhang, 2010)	Z-2010	587.9 ms	15.5% << SHA1	40 chars hash
Cognitive-based CAPTCHA system (Gossweiler et al., 2009)	G-2009	N/A	N/A	N/A
Graphical Captcha Authentication without Password Table (Juang et al., 2008)	J-2008	N/A	N/A	N/A
Authentication by Encrypted Negative Password (Lv et al., 2016)	L-2016	587.9 ms	15.5% << SHA1	64 chars hash
MD5 Hash SMS One-time Password (McLoone & McCanny, 2003)	M-2003	881.7 ms	7.6% << SHA1	32 chars hash
Securing passwords with CAPTCHA hash over web (Das et al., 2004)	D-2004	881.7 ms	7.6% << SHA1	32 chars hash
Improved Security Captcha Hash Encrypted [our proposal]	Proposed	**587.9 ms**	**Faster than others**	**40 char s hash**

Analyzing our method shows preference among others for preventing hacker's database attack from retrieving unauthorized details. Our approach password database solved the common password table clean for reading that aren't using encryption techniques (Das et al., 2007) as well as our usage of CAPTCHA's verification combined for protection against brute force (Ali & Karim, 2014), network folding attacks and DDoS problems (Saini & Anju, 2013). Other systems used crypto accessing algorithms without CAPTCHA verification, which is a weakness solved. We adopted sound CAPTCHA alphabets to provide opportunity to confirm text writing, that should be typed as CAPTCHA verification text, as CAPTCHA can be requested to be refreshed if completely unclear. Our system can be further used by PHP developers for authentication of privacy login passwords adopting encrypted keys (Ahn et al., 2003). The security testing of the system is remarked through the input login information on online web.

Figure 7, shows our proposed methodology graphical CAPTCHA to illustrate this usability feature. This contradiction between distortion and robotic guessing made our proposed methodology have less distorted CAPTCHA images, but protected combining cryptography and hashing (Alotaibi et al., 2019) different than HSV colour space image security (Hassan & Gutub, 2022). Table 4 shows our list of images with user selection speed for proper CAPTCHA images.

Figure 7. Example of proposed methodology CAPTCHA to illustrate usability feature

The proposed strategy implements a comprehensive encryption technique of AES cryptography beside Hashing, which gives a more effective edge to the authentication process. Table 4 shows how all techniques are evaluated for protection, integration and complexity, as marked between low level valued 0, moderate as 1, standard as 2 and our high level as 3.

Table 4. Time consumption and complexity table vs security

Notation	Technique	Delay	Integration complexity	Attack Prevention
L-2005	Graphical Passwords Captcha - Primitive Based on Hard AI	Low	0	Relay attack Online guessing attack
C-2010	Secure Scheme for CAPTCHA-Based Cloud Authentication	Delay	1	Phishing attack Dictionary attack Guessing password attack
M-2009	Improved DROP security: hard AI cloud	Low	0	Password guessing attack
C-2014	Password- based identity authentication system	Moderat e	2	Dictionary attack
Z-2010	Online password sensor-based authentication	low	2	Offline dictionary attack
G-2009	Cognitive-based CAPTCHA system	High	0	Dictionary attack
J-2008	Graphical Captcha Authentication without Password Table	Moderate	0	DOS attack Impersonating attack
L-2016	Authentication by Encrypted Negative Password	Moderate	1	lookup table attack rainbow table attack
M-2003	MD5 Hash SMS One-time Password	Low	1	Password attack
D-2004	Securing passwords with CAPTCHA hash over web	low	2	Brute force attack Dictionary attack
Proposed	**Improved Security Captcha Hash Encrypted [our proposal]**	**Very low**	**3**	**Relay, Online guessing attack, Brute force & Dictionary attack DOS& Password attack**

Our research calculation performed SHA-256 divided into two steps. In steps 1, SHA-256 dose the pre-processing of the data, followed by round computations where the message is expanded according to it. Through padding, the expansion is accomplished adding extra 512 bits. This is briefed in equation (Alsaidi et al., 2019) below for our testing, where "t" represents the number of rounds, as clarified in depth in literature (Zhang et al., 2019).

$$W_t = \sigma_i^{\{256\}}(W_{t-2}) + W_{t-7} + \sigma_0^{\{256\}}(W_{t-15}) + W_{t-16} \qquad (1)$$

Figure 8 shows the whole computational tasks of the SHA-256. Each round of the SHA-256 can create 8 hash values. The characteristics of the hardware XOR components of the system caused representing the computation round of the SHA-256 algorithm affecting the performance of our engineering system as determined in two categories, Login time and Rate of successful logins, as discussed next.

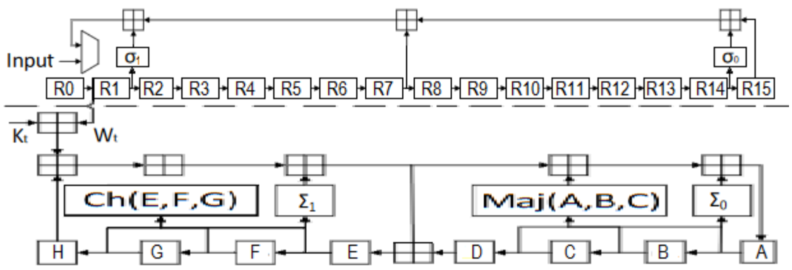

Figure 8. SHA-256 Computational scheme

Login time is analyzed by the total time needed by the user to login to the system. As this login time gets smaller as we ensure fast login. Accordingly, SHA-256 algorithm is chosen, as found to be fast in the hashing table by creating keys as used in (Bindu, 2015). On the other hand, the rate of successful login specifies the attempts made by the user to login to the system. This part shows the usability effect in the proposed system to help making the attempts easily accessible. Table 5 shows how relatively specific the performance of SHA-256 is.

Table 5. Performance of SHA-256

Design: SHA-256	Freq (MHz)	Delay (Cycles)	TP (Mbps)	Area (Slices)	Cost (TP/Area)
Basic	133.06	68	1009	1373 (12%)	0.735
2x-unrolled	73.975	38	996.7	2032 (18%)	0.491
4x-unrolled	40.833	23	908.9	2898 (26%)	0.314

COMPARATIVE ANALYSIS

The comparison is performed mainly to test the security insurance measures. Hence through deep studies of the previous work loopholes have been analyzed and the proposed approach has reached to present our 3-layers security architecture. Table 6 summaries the contributions, comparison of the advantages and disadvantages of the techniques, including our work

Table 6. Systems overall comparisons based on contribution, advantages and disadvantages

Technique	Contribution	Advantages	Disadvantages
V-2016	Audio captcha words	Visual impair users	Audio noise and vocabulary
A-2014	Puzzle captcha	Authentication security	Delay in solving puzzle captcha
C-2010	Dynamic CAPTCHA	Defend bots attack	Weak password against phishing
K-2016	Math CAPTCHA	Resists visual attacks	Complex delay login details
L-2016	Chinese CNN	Recognition accuracy	Low security
Z-2017	Vertical projection	Recognition accuracy	Low reliability
A-2003	Extended captcha	Secure cost-effective	High Risk of DOS attack
T-2014	Key exchange	Provide secure connection	Time delay and complexity
C-2014	Improved smart-card-based password authentication	Achieves mutual authentication	Complex delay login details
L-2005	Security enhancement for dynamic ID-based remote user authentication	No computational cost to improvements	Low reliability
J-2008	User authentication using smart card	Very low cost	Time delay and complexity
D-2007	ID-based remote user authentication	No need for password User can change and choose own password	Does not achieve mutual authentication and the secret key in the login phase
M-2003	New key scheduling method	Application to other encryption algorithms	Complex delay login details
M-2009	Vidoop CAPTCHA that relies on images	Avoid text-input	Recognition accuracy low/low reliability
G-2009	Identifying an image's upright position	Avoids text-input	Low reliability
Z-2019	Zhang's CAPTCHA via intelligent communication with RIA	Two line of defense	Time delay and complexity
Proposed	CAPTCHA based encrypted hash	Strong security & practical usability	Improve Hash function efficiency

Based on Table 6, Vaithyasubramanian (2016) research is only using audio-based CAPTCHA, which is beneficial to users who are visually affected, but may be not very convenient to all. As an overview, Table 7 below summarizes the comparison of promising techniques on basis of the essential authentication layers' availability and practicality.

Table 7. Authentication layers' availability and practicality evaluation

Notation	Technique	CAPTCHA	Hashing	Encryption	Usability
A-2014	visual CAPTCHAs and breaking of weak audio CAPTCHAs (Ali & Karim, 2014)	✓	✘	✘	✓
C-2010	CAPTCHA System Based on Puzzle (Cui et al., 2010)	✓	✘	✘	✘
K-2016	A non-OCR approach (Kaur, 2016)	✓	✘	✓	✘
A-2017	Modification based CAPTCHA (Althumaly & El-Alfy, 2017)	✓	✘	✓	✘
Proposed	Proposed Methodology	✓	✓	✓	✓

Table 7 comparison ensures that our engineering methodology can be applicable to enjoy various characteristics. We involve proper labeling for CAPTCHA images to be clear enough for the user to select images from the grid benefitting from all other schemes.

CONCLUSION

To ensure secure access to sensitive information is one fundamental challenge in today's e-platforms. Therefore, many techniques were proposed had some issues regarding security such as hacks that breach security and further modify sensitive information. This paper introduces an engineering methodology to protect the secure access to systems in convenient manner. We present combining graphical text-captcha, encryption, and hash function, building highest secure practical system. The testing of security shows resistance to protect against intelligent computer AI coding addressing bots cracking of password. The work involves graphical text-captcha for the user to select exact images from grids. The work tested graphical captcha to provide security against human guessing attacks as well as other common breaches. Future work suggested trying different CAPTCHA schemes, such as audio or video-based captcha, with more advanced encryption techniques. Further advanced Hash functions such as SHA3, can be tested aiming higher security, as believed coming e-platforms needing to mitigate improved hacker attacks, i.e. that need further unconventional anti-hacking refinement.

ACKNOWLEDGMENT

Special thanks to my genius graduate students of Computer Engineering course: Advanced Topics in Information Security (1400519), as their collaborative work remarked attractive contribution and completion used within this paper. Thanks to our great school, Umm Al-Qura University – Makkah, for supporting me by the sabbatical leave year (2022-2023) to focus working out this Cybersecurity research hoping to continue offering the MS graduate program as well as allowing for PhD, approved by Ministry of Education within Saudi Arabia, opening doors for progressive scientific activities.

Agreement: We declare that this work is original and not considered to be published in any other publication media.

Funding: There is no funding source.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent: Informed consent was obtained from all individual participants included in the study.

Conflict of Interest: The authors declare that they have no conflict of interest.

Data Availability: Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

REFERENCES

Ahmed, T., Tushar, K., Nova, S., & Rahman, M. 2016. Simple, Robust & User Friendly CAPTCHA 'InstaCap' for Web Security. International Journal of Hybrid Information Technology, 9(1): 163-182. https://www.earticle.net/Article/A268097

Ahn, L-V., Blum, M., Hopper, N., & Langford, J. 2003. CAPTCHA: Using hard AI problems for security. International conference on the theory and applications of cryptographic techniques pp. 294-311. http://doi.org/10.1007/3-540-39200-9_18

Alanizy, N., Alanizy, A., Baghoza, N., Al-Ghamdi, M., & Gutub, A. 2018. 3-Layer PC Text Security via Combining Compression, AES Cryptography 2LSB Image Steganography. Journal of Research in Engineering and Applied Sciences (JREAS), 3(4):118-124. https://doi.org/10.46565/jreas.2018.v03i04.001

Alassaf, N. & Gutub, A. 2019. Simulating Light-Weight-Cryptography Implementation for IoT Healthcare Data Security Applications. International Journal of E-Health and Medical Communications (IJEHMC), 10(4): 1-15. http://doi.org/10.4018/IJEHMC.2019100101

Al-Ghamdi, M., Al-Ghamdi, M., & Gutub, A. 2019. Security Enhancement of Shares Generation Process for Multimedia Counting-Based Secret-Sharing Technique. Multimedia Tools and Applications (MTAP), 78: 16283−16310. http://doi.org/10.1007/s11042-018-6977-2

Ali, F, & Karim, F. 2014. Development of CAPTCHA system based on puzzle. IEEE International Conference on Computer, Communications, and Control Technology (I4CT). https://doi.org/10.1109/I4CT.2014.6914219

Al-Juaid, N. & Gutub, A. 2019. Combining RSA and audio steganography on personal computers for enhancing security. SN Applied Sciences, 1:830. http://doi.org/10.1007/s42452-019-0875-8

Alkhudaydi, M. & Gutub, A. 2021. Securing Data via Cryptography and Arabic Text Steganography. SN Computer Science, 2(46). https://doi.org/10.1007/s42979-020-00438-y

Al-Nofaie, S. & Gutub, A. 2020. Utilizing pseudo-spaces to improve Arabic text steganography for multimedia data communications. Multimedia Tools and Applications (MTAP), 79:19−67. http://doi.org/10.1007/s11042-019-08025-x

Alotaibi, M., Al-hendi, D., Alroithy, B., Al-Ghamdi, M., & Gutub, A. 2019. Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination. Journal of Information Security and Cybercrimes Research (JISCR), 2(1): 9-20. http://dx.doi.org/10.26735/16587790.2019.001

Al-Roithy, B. & Gutub, A. 2021. Remodeling Randomness Prioritization to Boost-up Security of RGB Image Encryption. Multimedia Tools and Applications (MTAP), 80(18):28521–28581. https://doi.org/10.1007/s11042-021-11051-3

Alsaidi, A., Gutub, A., & Alkhodaidi, T. 2019. Cybercrime on Transportation Airline. Journal of Forensic Research, 10(4): 449. https://www.omicsonline.org/peer-reviewed/cybercrime-on-transportation-airline-109793.html

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

Al-Shaarani, F., Basakran, N., & Gutub, A. 2020. Sensing e-Banking Cybercrimes Vulnerabilities via Smart Information Sciences Strategies. RAS Engineering and Technology, 1(1): 1-9. https://drive.uqu.edu.sa/_/aagutub/files/Publication_Journals/2020_RAS_ET_Faiza_eBanking.pdf

Altalhi, S. & Gutub, A. 2021. A survey on predictions of cyber-attacks utilizing real-time twitter tracing recognition. Journal of Ambient Intelligence and Humanized Computing, 12(11):10209–10221. http://doi.org/10.1007/s12652-020-02789-z

Althamary, I., & El-Alfy, E-S. 2017. A more secure scheme for CAPTCHA-based authentication in cloud environment. IEEE International Conference on Information Technology (ICIT). https://doi.org/10.1109/ICITECH.2017.8080034

Bindu, C. 2015. Click based Graphical CAPTCHA to thwart spyware attack. IEEE International Advance Computing Conference (IACC). https://doi.org/10.1109/IADCC.2015.7154723

Chen, B-L., Kuo, W-C., & Wuu, L-C. 2014. Robust smart-card-based remote user password authentication scheme. International Journal of Communication Systems, 27(2): 377-389. https://doi.org/10.1002/dac.2368

Cui, J., Zhang, W-Z., Peng, Y., Liang, Y., Xiao, B., Mei, J-T., Zhang, D., & Wang, X. 2010. A 3-layer dynamic CAPTCHA implementation. IEEE International Workshop on Education Technology and Computer Science. https://doi.org/10.1109/ETCS.2010.575

Das, M., Saxena, A., & Gulati. V. 2007. A dynamic ID-based remote user authentication scheme. IEEE transactions on Consumer Electronics, 50(2): 629-631. https://doi.org/10.1109/TCE.2004.1309441

Gossweiler, R., Kamvar, M., & Baluja S. 2009. What's Up CAPTCHA? A CAPTCHA Based on Image Orientation. International conference on World wide web. pp.841-850. https://doi.org/10.1145/1526709.1526822

Gutub, A., Ghouti, L., Elarian, Y., Awaideh, S., & Alvi, A. 2010. Utilizing Diacritic Marks for Arabic Text Steganography. Kuwait Journal of Science & Engineering (KJSE), 37(1): 89-109.

Gutub, A., Al-Juaid, N., & Khan, E. 2019. Counting-Based Secret Sharing Technique for Multimedia Applications. Multimedia Tools and Applications, 78: 5591−5619. http://doi.org/10.1007/s11042-017-5293-6

Gutub, A. & Al-Qurashi, A. 2020. Secure Shares Generation via M-Blocks Partitioning for Counting-Based Secret Sharing. Journal of Engineering Research, 8(3): 91-117. http://doi.org/10.36909/jer.v8i3.8079

Hassan, F.S. & Gutub, A. 2022. Improving data hiding within colour images using hue component of HSV colour space. CAAI Transactions on Intelligence Technology, 7(1): 56–68. https://doi.org/10.1049/cit2.12053

Juang, W-S., Chen, S-T., & Liaw, H-T. 2008. Robust and efficient password-authenticated key agreement using smart cards. IEEE Transactions on Industrial Electronics, 55(6): 2551-2556. https://doi.org/10.1109/TIE.2008.921677

Kahri, F., Bouallegue, B., Machhout, M., & Tourki, R. 2013. An FPGA implementation and comparison of the SHA-256 and Blake-256. IEEE International Conference on Sciences and Techniques of Automatic Control & Computer Engineering-STA. https://doi.org/10.1109/STA.2013.6783122

Kaur, R. 2016. A non-OCR approach for math captcha design based on boolean algebra using digital gates to enhance web security. IEEE International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET). https://doi.org/10.1109/WiSPNET.2016.7566254

Kheshaifaty, N., & Gutub, A. 2020. Preventing Multiple Accessing Attacks via Efficient Integration of Captcha Crypto Hash Functions. International Journal of Computer Science and Network Security (IJCSNS), 20(9): 16-28. http://doi.org/10.22937/IJCSNS.2020.20.09.3

Kolekar, V., & Vaidya, M. 2015. Click and session based—Captcha as graphical password authentication schemes for smart phone and web. IEEE International Conference on Information Processing (ICIP). https://doi.org/10.1109/INFOP.2015.7489467

Kulkarni, P., & Malwatkar, G. 2015. The graphical security system by using CaRP. IEEE International Conference on Energy Systems and Applications. https://doi.org/10.1109/ICESA.2015.7503319

Liao, I-E., Lee, C-C., & Hwang, M. 2005. Security enhancement for a dynamic ID-based remote user authentication scheme. IEEE International Conference on Next Generation Web Services Practices (NWeSP'05). https://doi.org/10.1109/NWESP.2005.67

Lv, Y., Cai, F., Lin, D., & Cao, D. 2016. Chinese character CAPTCHA recognition based on convolution neural network. IEEE Congress on Evolutionary Computation (CEC). https://doi.org/10.1109/CEC.2016.7744412

Malutan, R., & Grosan, C. 2015. Web authentication methods using single sign on method and virtual keyboard. IEEE Conference Grid, Cloud & High Performance Computing in Science (ROLCG). https://doi.org/10.1109/ROLCG.2015.7367431

McLoone, M., & McCanny, J. 2003. High-performance FPGA implementation of DES using a novel method for implementing the key schedule. IEE Proceedings-Circuits, Devices and Systems, 150(5): 373-378. https://doi.org/10.1049/ip-cds:20030574

Merler, M., & Jacob, J. 2009. Breaking an Image based CAPTCHA. Technical Paper submitted to the Department of Computer Science, Columbia University, USA. http://www.cs.columbia.edu/~mmerler/project/Final%20Report.pdf

Saini, B., & Bala, A. 2013. A Review of Bot Protection using CAPTCHA for Web Security. IOSR Journal of Computer Engineering (IOSR-JCE), 8(6): 36-42. http://doi.org/10.9790/0661-0863642

Samkari, H., & 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. http://doi.org/10.5281/zenodo.3543455

Shambour, M.K. & Gutub, A. 2022. Progress of IoT Research Technologies and Applications Serving Hajj and Umrah. Arabian Journal for Science and Engineering (AJSE), 47(2): 1253–1273. https://doi.org/10.1007/s13369-021-05838-7

Shimazaki, K., Aoki, T., Hatano, T., Otsuka, T., Miyazaki, A., Tsuda, T., & Togawa, N. 2016. Hash-table and balanced-tree based FIB architecture for CCN routers. IEEE International SoC Design Conference (ISOCC). https://doi.org/10.1109/ISOCC.2016.7799736

Tirthani, N., & Ganesan, R. 2014. Data Security in Cloud Architecture Based on Diffie Hellman and Elliptical Curve Cryptography. IACR Cryptol. ePrint Arch. pp. 49. http://eprint.iacr.org/2014/049

Vaithyasubramanian, S. 2016. Review on development of some strong visual CAPTCHAs and breaking of weak audio CAPTCHAs. IEEE International Conference on Information Communication and Embedded Systems (ICICES). https://doi.org/10.1109/ICICES.2016.7518939

Zhang, W. 2010. Zhang's CAPTCHA Architecture Based on Intelligent Interaction via RIA. IEEE International Conference on Computer Engineering and Technology. https://doi.org/10.1109/ICCET.2010.5486295

Zhang, L., Xie, Y., Luan, X., & He, J. 2017. Captcha automatic segmentation and recognition based on improved vertical projection. IEEE International Conference on Communication Software and Networks (ICCSN). http://doi.org/10.1109/ICCSN.2017.8230294

Zhang, X., Wu, R., Wang, M., & Wang, L. 2019. A high-performance parallel computation hardware architecture in asic of sha-256 hash. IEEE International Conference on Advanced Communication Technology (ICACT). http://doi.org/10.23919/ICACT.2019.8701906