Design and Implementation Digital Invitation System Based on Secure Hash Algorithm 3

https://doi.org/10.3991/ijoe.v19i05.37583

Ismael Abdul Sattar Jabbar(✉), Hassan Kassim Albahadilyr, Alaa A. Jabbar Altaay
College of Science, Computer Department, University of Mustansiriyah, Baghdad, Iraq
ismaelabdul@uomustansiriyah.edu.iq

Abstract—Digital invitation system become one of the important systems due to the pandemic consequences specially in E-learning domains. The digital invitation needed to be secure enough for several reasons specially in the user demands. In this paper designed and implemented a digital invitation system based on secure hash algorithm which achieving multilevel of security. The first security level, that is the hash code generated for the digital invitation link used in the encryption process not only for the invitation date but also for the invitation time. on the other hand, the second security level achieved through out using the hash code as map for the hiding mechanism. The generated hash will be used for the data integrity as well. The proposed system evaluating the final stego-image as digital invitation using PSNR metric and the maximum value reach 64.28 while the minimum value reach 58.21.

Keywords—invitation system, hash function, SHA-512 algorithm, database, stego-systems

1 Introduction

Digital meet link generator used in a various field for different purposes in learning link generated digital links by "Google" used in Meet as well as in classroom. The digital link could be generated in secure mechanisms [1, 2]. The digital meet link generated allow users to communicate straight and efficiently which is not only very fast and light but also many participants can be followed [3]. links could be used to achieve secure meeting that's the build and implement a secure invitation system become in need. The security levels required in the invitation system based on the purpose and the end user demands [4, 5]. The data hiding in digital media, steganography and watermarking, is art that aims to conceal secret data into cover to intent of identification, copyright protection, and annotation. The main constraint factors of this operation are message data quantity, necessity of invariability of embedded data under distortions like lossy compression, third party removal, or modification. There are three categories of Data hiding techniques cryptography, steganography, and watermarking [6–8]. Watermarking and particularly steganography tends to embedded presence of hidden data while cryptography makes data gibberish. Data hiding techniques are differing from encryption techniques as they try to make the embedded data is unrecoverable and inviolate-able [9, 10]. There are different digital data hiding classes such as embedding copyright information in different digital media formats text, audio, image, or video with least possible perceivable degradation effects on the host signals. For example, effects must be inaudible or invisible to its observers. Hidden data quantity and data invariance to manipulation requires different embedment methodologies and as far as no single method is able to reach all of the goals then various classes of techniques are needed to coverage all ranges of applications. Main usages of digital media data hiding techniques are assuring content integrity and preserving copyright. To reach this objectives, embedded data should be preserved hidden in host signal even if is subject of degrading operations such as compression, lossy data, re-sampling, or filtering. The embedded data are in favor of both parties (author and consumer). So must be invariant against removal or detection. Technically, data hiding has enormous challenges. Important factor to achieve successful data hiding technique is to find places which are not convenient to be used by compression algorithms. The main challenge is filling data in this kind of places in a way that is not easy for compression algorithms to use it. An enhanced challenge is filling the holes in a manner that remains invariant against signal transformation in wide scale. Following features and restrictions are the criteria which a data embedding algorithm must meet [11]:

- Quality of host signal should not be degraded objectionably and the perceptibility of embedded data must be kept minimal.
- The data must be embedded into whole body of the target media rather than wrapper or header. Therefore, it would be kept intact in different formats.
- The data must be secure against intentional and intelligent removal attempts such as filtering, encoding, cropping, channel noise, lossy-compressing, re-sampling, scanning and printing, digital to analog (D/A) conversion, analog to digital (A/D) conversion, and etc.
- Since data hiding goal is to keep the embedded data into host signal, embedded data asymmetrical encoding is desirable feature but not essential.
- To guaranty data integrity error correction coding is necessary. Degradation of embedded data at signal modification time is unavoidable.

Arbitrary re-entrant and self-clocking are mandatory properties of the embedded data. These properties are to guaranty that embedded data will be retrievable even if only some fragments of the host be available. As shown in Figure 1, important steganography measurements are as follow:

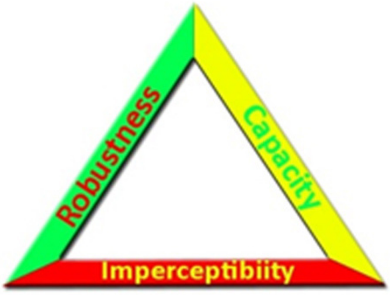

Fig. 1. Measurement triangle of steganography

A. Capacity

Capacity is the maximum amount of secret data can be embedded in a cover file. Capacity either can be defined as an absolute value in term of number of bits for particular cover or as a relative number regarding necessary bits to save final stego-file. Capacity value depends on both embedding function and cover file properties [12].

B. Imperceptibility

Stego object should not have important perceptual artifact. The higher fidelity of stego object, will give the better imperceptibility. This property would be satisfied if difference of resultant stego file be not distinguishable from original cover for warden [13].

C. Robustness

Robustness is property of harness of eliminating secret information from stego file. While detection of embedded secret data has much higher importance than its removal, but property of robustness talks about resisting against intentional distortion of communication channel by means of systematic interface or channel noise aiming to ban use of steganography techniques [14–16].

Robustness of steganography methods also can be examined through steganalysis attacks. Challenging aim of steganalysis is detection of existence of the secret message in cover file. Today numerous methods exist which can conduct steganalysis to reveal existence of secret information especially when the cover file is digital image. However, famous steganalysis approaches are as follow [17]:

- Visual detection
- Histogram analysis (detecting according first order statistics)
- Twofold statistical techniques for images by using spatial correlations
- Higher order statistics
- Steganalysis of JPEG files' compatibility
- Universal blind detection methods

The Secure Hash Algorithm 3 (SHA-3) is a family of six hash functions (SHA-224, SHA-256, SHA-384, SHA-512, SHAKE128, SHAKE256), based on new technology called sponge construction. this function also known as Keccak algorithm. SHA3-512 is developed and recommended by NIST. This algorithm accepting 512 bits as input and generate random mapping from string of data into a fixed size text. It is one-way hash function; this means that it is not possible to generate the plain text from the generated hash text. It is very powerful algorithm against security attacks and has a high-level security. It is collision resistance (cannot be generate same output for different input). It is used for digital signature authentication, pseudo random function and several security purposes especially in verification because the Same input generates same output. The algorithm is shown in the Figure 2. The steps of the SHA3 algorithm illustrated in the following:

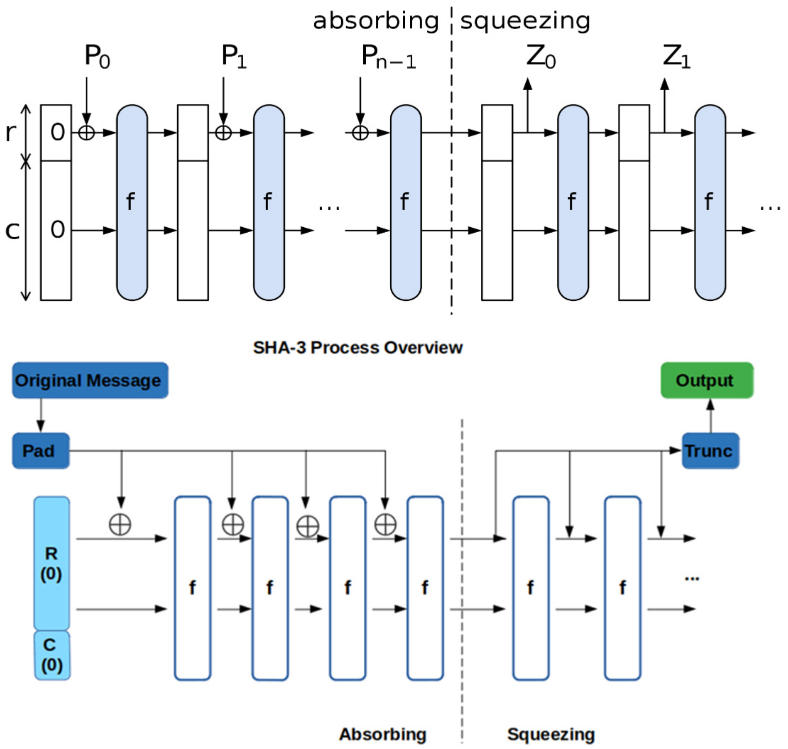

Fig. 2. Absorbing and squeezing in SHA3 algorithm

In the absorbing phase, the algorithm taking message's blocks and performing operation XOR with the subset of state and transformed using permutation. In the squeeze phase, output blocks read from the subset alternated with transformation function.

The size of the part state called rate "r"

And the unattached part called capacity "c"

The SHA-3 algorithm has new interesting designs with unique features. Like ability of running efficiently on a wide variety of platforms, and using parallelism. The capacity determining the security of scheme. The SHA algorithm using in a lot of places, as follows:

1. Digital Signature Verification.
2. Password Hashing.
3. SSL Handshake.
4. Integrity Checks.

2 Proposed system

The following Figure 3 shows the proposed system digital invitation system. At the first step the sender (inviter) determines his account with available attached services the reach the possible invitation links database could be used with sender account, second date and time for the digital meeting, third the set of targeting accounts invitees "I" out of the available domain user's database related to inviters. account, such that $I \geq S$. Digital link selected randomly out of links database and encryption process achieved based on the algorithm (1).

Input	Date=D, Time=T, Invitation link=IV
Output	Encrypted Date and time C_D, C_T
Process	1. Obtain Hash code "*h*" for Invitation link =IV based on SHA3-512. Such that, $\boldsymbol{h} = \mathbf{SHA}3-512(\mathbf{IV})$ 2. Encrypt Date *D* and time *T* based on the hash code obtained from step1. Such that, $\boldsymbol{C_D} = \boldsymbol{h} \oplus \boldsymbol{D}$ and $\boldsymbol{C_T} = \boldsymbol{h} \oplus \boldsymbol{T}$.

The invitation link will be hidden inside a cover image of type "RGB" that is randomly selected form database cover images, while the encrypted date and time will be hidden inside the cove image also. The generated hash code using SHA3-512 algorithm will be attached as digital signature with in digital invitation. The stego image will represent the invitation which is contains the invitation link as well as the encrypted date and time and digitally singed with SHA3-512 hash. Such invitation will be sent to the set of target users *I*, where they are already selected out of database *S*.

Let, $x_1, x_2, \ldots . x_{n-1}, x_n$ a set of invitees that already selected by sender from available user database each one in this set will receives digital invitation *DI* which is generated by sender δ. The digital invitations will be stego image and with digital signature using SHA3-512 algorithm.

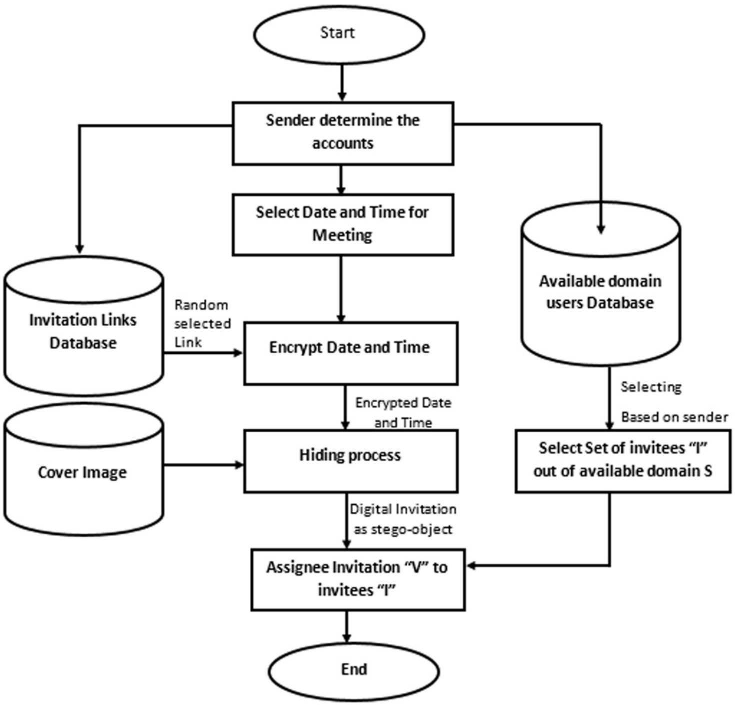
Start
Sender determine the accounts
Select Date and Time for Meeting
Available domain users Database
Invitation Links Database
Random selected Link
Encrypt Date and Time
Selecting Based on sender
Encrypted Date and Time
Cover Image
Hiding process
Select Set of invitees "I" out of available domain S
Digital Invitation as stego-object
Assignee Invitation "V" to invitees "I"
End

Fig. 3. Proposed system digital invitation system

The hash code generated will achieves the integrity goals for the security purpose. The digital invitation will be in the form of

1. Stego image.
2. SHA3-512 Hash code.

At the receivers' sides will get the digital invitation and try to extract the digital link as well as date and time based on the extracting algorithm and decryption algorithm. If the hashed extracted link doesn't match the digital signature hash using SHA3-512 Algorithm this will rise issues and achieves data integrity. The integrity process can be done as shown in Figure 4.

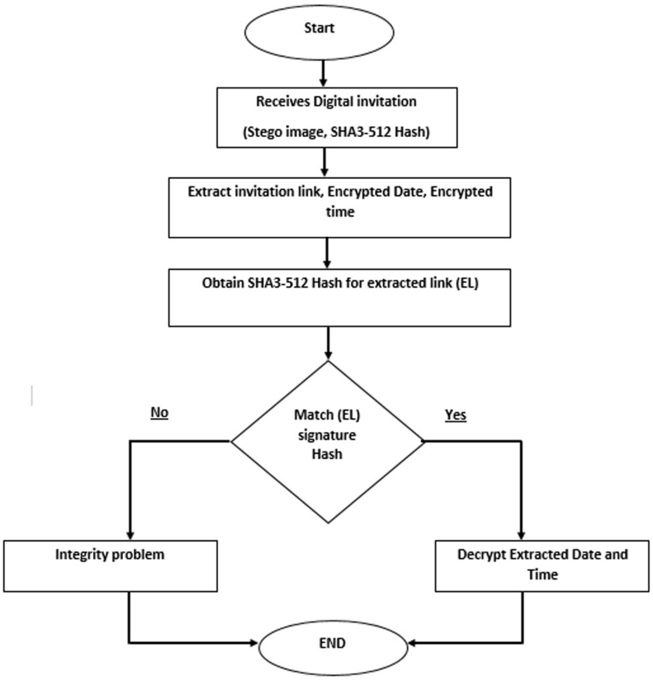
Start
Receives Digital invitation
(Stego image, SHA3-512 Hash)
Extract invitation link, Encrypted Date, Encrypted time
Obtain SHA3-512 Hash for extracted link (EL)
No
Match (EL) signature Hash
Yes
Integrity problem
Decrypt Extracted Date and Time
END

Fig. 4. Integrity process flowchart

Proposed hiding algorithm in the invitation system to achieve secure invitation the proposed algorithm as shown below:

Input	Cover Image (CI), Encrypted Date and time C_D, C_T, Invitation link =IV, Hash code 512
Output	Stego-image (Digital Invitation)
Process	1. Start 2. Targeting hiding pixel bits' trough SHA3-512 hash based on following steps: (a). Since hash 512 length then to address four locations in a pixel needs 2 bits, thus $x = 512/2 = 256$ locations. (b). Use the 256 obtained from (a) to hide activation link (IV), Encrypted Date and time C_D, C_T. 3. After finish all bit for hiding process form the stego-image. 4. End.

The 512 hash bits will give 256 locations $\boldsymbol{x} = \mathbf{512/2} = \mathbf{256}$ to address one of four LSB bits in a pixel as shown in the Figure 5.

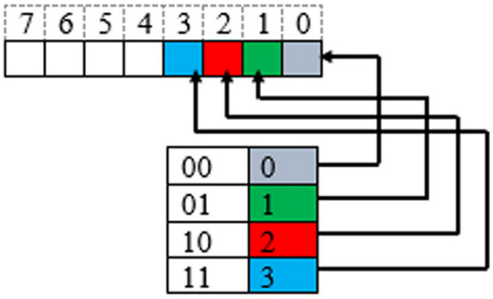

Fig. 5. Hiding process addressing

The 256 bit could hide 51 digit of encoding secret message (Invitation link, Date, and time) as $y = 256/5 = 51$. Because the invitation link is 10 digits' length, the date length of 8 digits and time of 1-digit length totally 19 digits, thus the hash code will be sufficient to be used for hiding process and making the proposed system working fast due to the limited length of the secret information.

The extracting process can be shown by the following proposed algorithm

Input	Stego-image (Digital Invitation)
Output	Encrypted Date and time C_D, C_T, Invitation link =IV
Process	1. Start 2. Read secret message bits from the Stego-image based on SHA3-512 hash code. 3. Gather all secrets bits to form the Invitation link (IV), Encrypted Date and time C_D, C_T. 4. End.

After getting the secret message bits that represents invitation links as well as encrypted date and time, the next step at the receiver side is the decrypting process to find out the date and time for the invitation. The decryption process achieved with algorithm.

Input	Encrypted Date and time C_D, C_T, Invitation link =IV
Output	Date=D, Time=T
Process	1. Obtain Hash code "*h*" for Invitation link =IV based on SHA3-512. Such that, $\boldsymbol{h} = \mathbf{SHA3-512(IV)}$. 2. Decrypt Date C_D and time C_T based on the hash code obtained from step1. Such that, $\boldsymbol{D} = \boldsymbol{h} \oplus \boldsymbol{C_D}$ and $\boldsymbol{T} = \boldsymbol{h} \oplus \boldsymbol{C_T}$. 3. End.

3 Results and discussion

The proposed system run to produce 10 invites for meeting could hold on 18/06/2022 with time 10 (time considered 24 hour). The ten digital invitation link randomly selected from the available invitation link database, Thus the link works as input for SHA3-512 Algorithm to produce 128 hex digit which offering 512 binary bits, the hash code shown with Table 1.

Table 1. Hash code generated using SHA3-512 algorithm

NO:.	Digital Invitation Link	Date	Time (24)	SHA3-512 Hash
1	mbv-qoke-jgp	18/06/2022	10	e86570864a1934793ab389ded397cd187acfdec642993797d3c3812ef998ca5158ba2c94795c17b4bc27c4a372985041cafdc57ff5a34a0c37f243b552dad793
2	ays-equw-qny		10	198a8a1bc01209f5db737eb23784b409ebf5c356e1b5b66301d2dec22dfed01104e4a90da3d0ead4dd53171b07b48707918be755070fda77dc5bc127aca8c98d
3	dwf-nchr-ecr		10	af81f38347ca997e6a1b591ebb164f19c4d5f46ec580c8e90de5a372c0cf6f8f2377971aa944889b74e99e8ca24ca60159c36e0e7479693f8fe2d975f6f448d0
4	twr-ysmc-bje		10	d2c1462d8e034d077bd2e7d6c8740a86edf8cc99ccd30d747736f93de64c8fa4d3a6f590fac17949982556295206a28d35ac56eedd684dae84b8b8114fbc1e42
5	fpt-vibh-dvu		10	2d2780cc3f4c37c977e3130daca679cc6f7fe555c587cb88a04b408148520b3ced8867042e11e5c420a85fa6fd5ef87ee01fc5f1832b4b3855b78bbc50244240
6	onk-hijq-ndz		10	ffced65de058a3f5c7bc7901fd432d44c1990392e8647aa646dafc260f7482f7b382be0eab6f8de20f62d8d691a59969d8498d9cccc552512c01ce70d06c70f4
7	ggq-vjff-zmt		10	a92768adbe3fa58e658821d918cdea16d5194346fe1a4fb21ba92004b8b214fbf095a6239e5a9ccb97d9d380d14f497224a270be4a58598c09432faf00bfe605
8	yio-reug-pqp		10	f4295d390c3e7fe94dc0cedb291ad1e9bc91f12cdf23271a09883cab16ec63c9889c3b31fd2f9dabbaf82af372558447e427a7b6b457cf41b171e1a0822456ce
9	okr-mgfc-ibk cpz-kdxr-xns		10	72a3ab358168ad30fe5fad80d0e2ad531ac48a62aa81562e876e32d50249d7a80289a0c0dff527739bcf06de6001d37e6dabedda16d210cdb39f22ce28ecd656
10			10	6e76f6af88c106811a86a226484b9a3ca9b0beea48256a283a3558f51b830305aebff4e4a20796a860dfb6b1ed43dec15f29c8a986c0c9c39cbf95f679161616

Each one of the 10 run could be used to produce digital invitation by encrypting data and time based on algorithm (1). The value of the PSNR used to measure the hiding process effectiveness, which is one of the common metric used. The result for PSNR to hiding process can be shown with following Table 2.

Table 2. It show that the result for PSNR to hiding process

Number of Run	Cover Image Size (Pixels)	Invitation Digital link	Date	Time	SHA3-512 Hash Code	Peak Signal to Noise Ratio (PSNR)
1	128*128	qul-uovr-esl	25/05/2022	10	a52d83b207406f5a2d7 63ed8d235c07c051fc1 b779f76338091e88c3cf 3b4cdd35cc69cfb558 62240819daea64226d7 fe5a99e877b8a85f9e3 783259374d6708	58.21
2	256*256	wat-byjy-nov	12/06/2022	12	1cf5e8055d5b21f5cf3c 4e9fe6ce838b095aaf8 271fe61657d22e4d4c 6d5796413e2048847c 3eb5b58fe234f7613 da00604c95c0b9819e 4a4536e3a6daa1bc56	59.4
3	300*300	zkb-iywr-vsi	09/06/2022	19	ca51d2dabd5cb82cf7 c205fb7bd7b5950 e4d20fa09fc313ed5 1e43e2559685e86f5 c430d7f6ae0c04c3c9 ff736ea8af2b12 bae6c85b17ea27b128 cc426862e38	60.43
4	512*512	utx-blpt-oqg	06/07/2022	06	0fc7c87995097cd71da 669202984b9f8a3 c4dd9ce2aa99bfe8b70 fb31a1d34c6568 c134f94ddb42956555b 186f678d7b26bf947 f58881a2dc64c1de153 5d8a9a	61.54
5	1024*1024	tcv-uptu-vdb	17/08/2022	21	8d0c5ba042f8a70f0781 f3e0d8550378f479d65 7aea00d73f48640438 5c00a1d5932484bfc 8b6110e5ab18e920d 2c67663ae4d1a4735c f72f8efdd13a800bfe4	64.28

The proposed invitation system must be tested to work online or in real time environments, thus such system has to consider time consumption for providing the secure invitations the Figure 6.

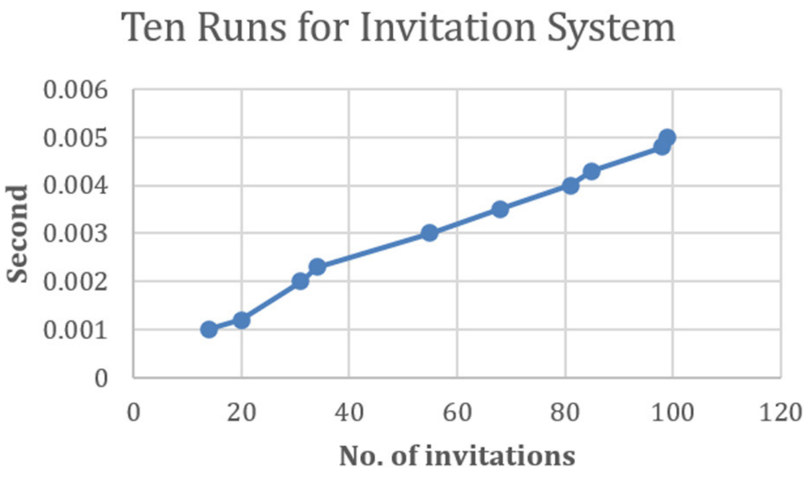

Fig. 6. Proposed system with time consumption

The Figure 6 clearly showing that when the number of invitations increased the time consumption also increased the proposed system can produce 100 invitations within 0.005 second.

4 Conclusion

Invitation system one of the important applications become in needs for different aspects. The proposed system contains multilevel of security utilizing the hash function which is one-way function as well as fast to compute the SHA-512 used to provide a good length used in the hiding process as well as achieving the integrity of data. Also, the proposed system can work well as real time system to provide secure invitations. As the time and date will be used in the invitation system that will be another complexity add to the security levels of the proposed digital invitation system.

5 References

[1] I. A. S. Jabbar, S. H. Shaker, and M. N. Abdullah, "Database Meet Link Generator Based On Linear Feedback Shift Register and Message Digest Algorithm," *Webology*, pp. 2236–2243, 2022.

[2] I. A. A. Jaafar Q. Kadhim, Haider T. H., and Salim ALRikabi, "Enhancement of Online Education in Engineering College Based on Mobile Wireless Communication Networks and IOT," *International Journal of Emerging Technologies in Learning (iJET)*, vol. 18, no. 01, 2023. https://doi.org/10.3991/ijet.v18i01.35987

[3] A. Aswir, M. S. Hadi, and F. R. Dewi, "Google Meet Application As An Online Learning Media for Descriptive Text Material," *Jurnal Studi Guru Dan Pembelajaran*, vol. 4, no. 1, pp. 189–194, 2021. https://doi.org/10.30605/jsgp.3.3.2020.533

[4] H. T. Hazim, "Secure Chaos of 5G Wireless Communication System Based on IOT Applications," *International Journal of Online & Biomedical Engineering*, vol. 18, no. 12, 2022. https://doi.org/10.3991/ijoe.v18i12.33817

[5] H. Tauma and H. Salim, "Enhanced Data Security of Communication System using Combined Encryption and Steganography," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, pp. 144–157, 2021. https://doi.org/10.3991/ijim.v15i16.24557

[6] R. A. Azeez, M. K. Abdul-Hussein, and M. S. Mahdi, "Design A System for An Approved Video Copyright Over Cloud Based on Biometric Iris and Random Walk Generator Using Water-Mark Technique," *Periodicals of Engineering Natural Sciences*, vol. 10, no. 1, pp. 178–187, 2021. https://doi.org/10.21533/pen.v10i1.2577

[7] I. A. Aljazaery and M. R. Aziz, "Combination of Hiding and Encryption for Data Security," *International Journal of Interactive Mobile Technologies*, vol. 14, no. 9, pp. 34–47, 2020. https://doi.org/10.3991/ijim.v14i09.14173

[8] A. H. M. Alaidi, R. a. M. Al_airaji, I. A. Aljazaery, and S. H. Abbood, "Dark Web Illegal Activities Crawling and Classifying Using Data Mining Techniques," *International Journal of Interactive Mobile Technologies*, vol. 16, no. 10, 2022. https://doi.org/10.3991/ijim.v16i10.30209

[9] I. A. Aljazaery, "Encryption of Color Image Based on DNA Strand and Exponential Factor," *International Journal of Interactive Mobile Technologies (iJIM)*, 2021.

[10] O. Yahya and I. Aljazaery, "Reducing the Data Rate in Internet of Things Applications By Using Wireless Sensor Network," *International Journal of Online & Biomedical Engineering*, vol. 16, no. 03, 2020. https://doi.org/10.3991/ijoe.v16i03.13021

[11] A. A. J. Altaay, S. B. Sahib, and M. Zamani, "An introduction to image steganography techniques," *in 2012 International Conference on Advanced Computer Science Applications and Technologies (ACSAT)*, IEEE, pp. 122–126, 2012. https://doi.org/10.1109/ACSAT.2012.25

[12] H. B. Kekre, A. Athawale, B. S. Rao, and U. Athawale, "Increasing the capacity of the cover audio signal by using multiple LSBs for information hiding," *in 2010 3rd International Conference on Emerging Trends in Engineering and Technology*, IEEE, pp. 196–201, 2010. https://doi.org/10.1109/ICETET.2010.118

[13] A. A. J. Al-Taay, S. B. Sahib, and M. Zamani, "Multimedia Data Hiding Evaluation Metrics," *Recent Researches in Information Science and Applications. WSEAS*, vol. 2, pp. 29–34, 2013.

[14] T. Morkel, J. H. Eloff, and M. S. Olivier, "An Overview of Image Steganography," in *ISSA*, vol. 1, no. 2, pp. 1–11, 2005.

[15] A. Bouguessa, N. H. Said, and A. A. Pacha, "New Technique of Steganography Based on the Theory of Chaos: A Survey," *Malaysian Journal of Computing and Applied Mathematics*, vol. 4, no. 1, pp. 1–12, 2021.

[16] N. Alseelawi, H. T. Hazim, and H. T. Salim ALRikabi, "A Novel Method of Multimodal Medical Image Fusion Based on Hybrid Approach of NSCT and DTCWT," *International Journal of Online & Biomedical Engineering*, vol. 18, no. 3, 2022. https://doi.org/10.3991/ijoe.v18i03.28011

[17] A. Jabbar, S. Sahib, and M. Zamani, "An introduction to watermarking techniques," *in 12th WSEAS International Conference on Applications of Computer Engineering (ACE 2013)*, Cambridge, MA, USA, January, 2013.

6 Authors

Ismael Abdul Sattar Jabbar, is a Ph.D holder in computer science from Informatics Institute for postgraduate studies. He gets M.Sc. degree in computer science from Delhi University, Faculty of Mathematical Sciences in 2012; B.Sc. degree in computer science in 2006 from Al-Mustansiriyah University, Collage of Science. He has published more than 17 research papers in national or international journals and conferences with 7 books in various fields in computer science.

Hassan Kassim Albahadilyr, College of Science, Computer Department, University of Mustansiriyah, Baghdad, Iraq.

Alaa A. Jabbar Altaay, College of Science, Computer Department, University of Mustansiriyah, Baghdad, Iraq.

Article submitted 2022-12-17. Resubmitted 2023-01-22. Final acceptance 2023-01-24. Final version published as submitted by the authors.