A Novel approach towards Implicit Authentication System by using Multi-share visual key Cryptography Mechanism

Dr. Ajay B. Gadicha¹, Dr. Vijay B Gadicha², Ahmed J. Obaid³

¹Head and Associate Professor, Department of Computer Science and Engineering P.R. Pote College of Engineering and Management Amravati (Maharashtra), India.
² Associate Professor, Department of Computer Science and Engineering G H Raisoni University, Amravati.
³ Faculty of Computer Science and Mathematics University of Kufa, Iraq

ajjugadicha@gmail.com
vijay.gadicha@raisoni.net
ahmedj.aljanaby@uokufa.edu.iq

Abstract: Currently huge amount of data used to stored, extracted and transacted via various stand alone and internet based applications. These applications are extended towards the verticals like huge databases, data warehouses, cloud computing services and various client-server applications. In all these applications important data used to float day in day out. Therefore preserving user authentication & access control is extremely important aspect of information security. Here an attempt is made to generate an implicit authentication system using multi-share visual key cryptography which will generate strong password keys by using images. Initially various images will be fused to form a resultant image than on this fused visual key cryptography will be performed which will provide multiple shares, out of these one of the share is selected to generate strong password strings/keys to accomplish the task of access control or user authentications.

Keywords: Data confidentiality, databases, data warehouses, cloud computing services, Cryptography, Cipher Text.

1. Introduction

Information Security is one of the essential parameter to follow in this computer based communication world. All the computer users, internet users or users which are involved in data communication cannot deny the importance of the information security. Information Security can be provided to the secrete information by using the aspects like data confidentiality, valid user authentication, data integrity. Let us consider scenario where two users wants to communicate securely over a completely insecure channel. Where an intruder or hacker may read intercept, modify, or perform some computations on the data which has been transmitted between the transmitter and receiver. In this scenario to preserve the information security following properties may be indentified so that secure communication will be established.
Figure1:- Fundamentals of Information Security

1.1 Confidentiality:-

The sender of data and only intended receiver should be able to understand the actual context of the transmitted message because intruders may intercept the message. Here this is needful that the plain text message must be encrypted so that an intercepted message can’t be decrypted by the intruder. This terminology can be typically termed as data secrecy or data confidentiality. This concept of data confidentiality is commonly used for establishing secure communication between the two communicating parties. To achieve the data confidentiality cryptography is used which is nothing but a process to convert a plain text in its corresponding cipher text by using some suitable encryption algorithm and the needful key values. Once the cryptography is perform on the given plain text it will results in cipher text which is a meaningless text so even if an intruder get this text still he/she don’t understand completely until he/she knows its corresponding decrypting process.

1.2 Authentication:-

Here both the sender & receiver want to confirm the identities of each other over communication channel. To confirm each other identity face to face is very easy because human visual reorganization solve this problem but when communication is over a medium or a channel where both the communicating parties physically a part their establishing authentication is not so simple. Usually when sender and receiver are physically apart and want to make sure about each other identity then authentication is done solely on the basis of messages or data exchange between the two parties. By those messages or corresponding data communicating parties used to uniquely identify each other. Generally, authentication methods are classified into three categories:

1.3 Data Integrity:-

Even though the two communicating parties on a computer network or internet authenticate each other but still they need to make sure that the contents of actual communication are not modified altered or copied by someone while data is being transmitted from sender to receiver this phenomenon is called data integrity. Various checksum methods can be identified to check the integrity of original data [Xiaotian Wu and Wei Sun][36]

1.4 Visual Key Cryptography:
Basically, Cryptography is a technique in which known plain text can be converted into some Cipher text by using encryption algorithm and appropriate key value. These cipher texts are formed to ensure the secrecy and confidentiality of the information. Because the cipher text generated after the implementation of cryptography is not easily understandable, actually it’s a meaningless text which is encrypted by using some algorithm.

\[ \text{Plain Text} \xrightarrow{\text{Encryption Algorithm}} \text{Cipher Text} \]

**Figure 2:** Cryptography

To analyze the strength of a cipher text is important because it’s subjected to various kinds of attacks. The field of cryptology, which is also known as cryptanalysis ensures that the strength of cipher text must remain strong enough to defend against all kinds of known attacks. In modern age various cryptographic algorithms are developed but an end-to-end information security will be only ensured once they are deployed properly on the given plain text information.

Basically cryptography is used to convert the data from one form to another. In cryptography there is a technique that is visual cryptography in which secret image which needs to be hide will get converted into number of images known as shares. Where VC is different than any other traditional cryptography techniques because in visual cryptography it does not required any complex computations during the decryption of the secret image. In visual cryptography the secret image will be obtained or decrypted by stacking all the shares together. The main advantage of the visual cryptography is if anyone capture the share then from a single share would not be revealed anything related to data.

2. Literature Review:

As per the detailed literature survey done associated to information security, it is observed that currently in this Internet based communicating world there is fundamental requirement of information security to safeguard our secret information. Information security is a huge challenge as per as e-commerce, e-transaction, e-business, and other electronic transformation of information is concern and no individual will deny this fact. Information security fundamentally can be implemented over three different verticals, namely data confidentiality, user authentication/access control and data integrity. Current research work is dedicated to achieve user authentication by generating strong passwords.

Fundamentally to establish the user authentication the communicating parties over a given channel of communication have to prove each other’s identity. To do this work the simplest and oldest method which is used is password. Basically passwords are alphanumeric characters which are utilized by a communicating party to verify its identity by a verifier (it may be a server, a process or a login application).once verifier confirms the identity of the communicating party then access is given to the respective party otherwise access is denied. In whole process of authentication it is very clear that the backbone of this system relies in the strength of the password used for proving user identity.

Basically cryptography is used to convert the data from one form to another. In cryptography there is a technique that is visual cryptography in which secret image which needs to be hide will get converted into number of images known as shares. Where VC is different than any other traditional cryptography techniques because in visual cryptography it does not required any complex computations during the decryption of the secret image. In visual cryptography the secret image will be obtained or
decrypted by stacking all the shares together. The main advantage of the visual cryptography is if anyone capture the share then from a single share would not be revealed anything related to data.

[Ilker Korkmaz and Mehmet Emin Dalkilic, 2010] proposed that, any password not only be private to its owner but also be chosen as not to be cracked easily by others. In authentication process of any critical system a strong password must be used which can’t be cracked easily by any unauthenticated persons. Therefore the strong password selection gets significance for the general system security. The proper and improper properties on password preferences are revealed via examining the real samples from this study. The method which is used in this work is first to gather the real passwords in plaintext, then to crack the encrypted forms of them and finally to examine statistical queries on those passwords in order to distinguish the common strong and weak characteristics.[15]

[Pradeep Kumar Sharma and Hari Mohan Singh, 2014] Generally the term cryptography is used to hide the original information and provides the security to the messages so that the unauthorized users are unable to access the information. Very first time cryptography is used to encrypt the plain text into the cipher text by using the unique key means data from original form get converted into some other form known as encrypted data. And at the other end that data is decrypted by using the same key or different key i.e. again data is converted into its original form. Most of the data is transfer over the network so it required some security to achieve the security various cryptography techniques were used, known as visual cryptography scheme. A new VCS approach and its implementation for a gray scale images which based on intensity division has been discussed. In this mechanism the intensity of pixels are divided into LSB’s and MSB’s. So, at the receiver’s side two shares are generated using MSB’s stacking of these provide the revealed image. The qualities of shared images are improved even after decryption of the secret image then finally it will get compared with the original image. The performance of the proposed approach is measured by calculating MSE values, PSNR values and histogram.

![Figure 3](image.png)

**Figure 3:** Sharing scheme for black and white image pixels.

In above given figure, it is observed that on the original secret image the two share visual cryptography is performed. This will generate two secret shares of the original image. When all these shares are stacked than the original secret image can be recovered.

[Bin Yu et al., 2007] When there is a need to share more than one secrete image then original visual cryptography scheme (VCS) fails, because at a time only single image can be shared by the original VCS. So, whenever there is need to share more secrete images for that there is a need to preserve a number of shares which increase our burden. A multi-secrete sharing threshold visual cryptography scheme is proposed which is based on (k, n)-VCS and that participant preserves a share to share more than one secrete image and also expands the scope of application.

[Bin Yu et al., 2008] A modified threshold visual cryptography scheme is proposed which based on (k, 1, n)-VCS, which evaluates the relationship between the pixel expansion and also analyze the range of the participants number. A more accurate description of multi secret sharing visual cryptography scheme is given which based on (k, 1, n)-VCS, that is a new method. After the analysis of the experimental results it is observed that both pixel expansion and relative difference of this method are better than the previously existing ones.
[Xiaotian Wu and Wei Sun, 2013] There is one method which used to implement visual key cryptography without doing any pixel expansion that is the Random grid (RG) method. In Random grid based visual cryptography due to the average light transmission of share is fixed at (1/2) because of which the lower visual quality of reconstructed secret image is reveal. In this proposed work, the concept of generalized Random grid was introduced, in which the light transmission of shares becomes adjustable, and also for implementation of different VC schemes generalized RG methods were adopted. A (2, 2) generalized RG based VC is the first basic algorithm which has to be devised. Mainly two VC schemes containing a (2, n) generalized RG based VC and another one is a (n, n) XOR-based meaningful VC are constructed. In VC some problems are occurred to overcome these problems two derived algorithms are designed. In the (2, n) scheme, the quality of recovered image is further improved. The management of shadows becomes more efficient by constructing the meaningful shares in the (n, n) method and also the chance of misgiving on secret image encryption is decreased. In addition, the quality of both the shares gets improved and also achieved recovered secret image.

[Xiao-Yi Liu et al., 2013] Here, an enhanced color visual cryptography is presented which is based on the modified visual cryptography mechanism. A color secret image can be shared by this scheme over one noise like share image and n-1 arbitrary natural images. The encryption process extracts the features of the images from each of the natural image rather than changing the contents of the original image. This mechanism can efficiently decrease the transmission risk and also solve the problems of management. Likewise, this method makes it possible to obtained secret image without any distortion and the pixel expansion problem is also avoided.

[Xiaotian Wu et al., 2014] To solve the problem of poor visual quality without darkening the background in VC, the XOR based visual cryptography methodology may be used. Here two XOR based algorithms are proposed, that is XOR based VC for general access structure that is known as GAS and another one is XOR based VC for adaptive region incrementing. The aim of the first algorithm is, using GAS complicated sharing strategy is implemented, during which it will also maintain the qualities such as no pixel expansion, no code book requirement is needed, and perfect reconstruction of secret is done. Whereas, the concept of adaptive security level is introduced in the second algorithm, in this instead of the quality of the stacked shares the security levels are recovered in accordance with the qualified sets. The adaptive region incrementing XOR based VC is then enriches the applications.

[Yanyan Han et al., 2014] A new digital watermarking algorithm of color image has proposed here. After processing a watermark, based on visual cryptography two shares are generated. One of them is protected by the copyright and another one is embedded into a color image. The proposed scheme is easily implacable and highly feasible. The robustness and the embedding capacity of watermark can be improved effectively using this mechanism.

[M. Desiha and Vishnu Kumar Kaliappan, 2015] Visual cryptography allows secret splitting strategy which is used to convert the secret image into number of shares. But because of some security issues in VCS it is not that much effective and not highly worth. Because of certain drawbacks occurs in VCS, extended visual cryptography was developed, in this the portion images are constructed to contain expressive cover image so that it will be useful in the biometric security techniques. Here, the effective dithering halftone technique was proposed for time reduction process on generating the halftone image and also useful for improving the visual quality of secret image. This mechanism provides the good security and the effective processing as compare to the existing VC approaches.

[Hsiang-Cheh Huang, Feng-Cheng Chang 2015] Basically visual cryptography provides the security of multimedia contents. Due to the huge amount of multimedia data transfer over the channels compression mechanism is essential part over there. Recently, compressed sensing is mainly used for the data compression because of its better performance. Few amounts of coefficients are capable to obtain the reconstructed image with acceptable quality in the case of compressed sensing. In compressed sensing, for protecting the ownership of the multimedia information, shares or the visual cryptography information is hided into the compressed sensing coefficients. Rather than focusing on the characteristics of the visual
cryptography, compressed sensing coefficients are divided into chunks for transferring over multiple channels. Here for protecting the ownership extracted shares can be verified. After the simulation results obtained it is observed that this mechanism can be applicable and it provides the enhance performance if the presented mechanism is combine with the robust visual cryptography. [Sruthy K Joseph and Ramesh R, 2015] In 1994 visual cryptography scheme was developed by Adi Shamir and Moni Naor. There are some drawbacks occurred in most of the visual cryptography schemes like pixel expansion, poor quality of reconstructed image, share management difficulty etc. So to overcome this drawback a visual cryptography scheme using random grids was proposed in which a common share is used to transmit n binary secrets. In (2, 2) binary visual cryptography scheme, the binary secret image is divided into two shares. In this mechanism, n+1 share images were used to transmit n secrets and extra share is their which is common to all the secrets.

Here the shares are generated without pixel expansion using random grid. The presented scheme can be seemed as a modified scheme of (2, 2) random grid based visual cryptography. As here, single share is used as a common share because of which network bandwidth utilization becomes more efficient. [K. Shankar and P. Eswaran, 2017] In the visual secret sharing scheme, it is difficult to expose any data on the original image without obtaining any single share. In fact, original image is obtained by overlapping the entire shares directly, whereas the human visual system is able to identify the secret image without using any complicated computational tools. That means if the numbers of shares are generated then the communication is done steadily. In this proposed work, elliptic curve cryptography mechanism is used to encrypt the generated shares.

Whereas a new innovative technique is used here for generating the multiple shares which are subjected to encryption and decryption. In this method shares are generated from the pixel values and these pixel values are extracted from the color image [24-28].

### 3. Proposed Work:

The visual cryptography is performed on obtained fused image which is fusion of various colored images. Following screenshot provides the details of various levels conducted to derive the secret share which ultimately going to provide the password string/key.
As per the screenshot#01 to achieve the access control, the visual key cryptography is applied on image dataset and result analysis is carried out.

Table 1: Visual Cryptography Analysis

| Image Name | MSE    | PSNR | Mean | Mean R | Mean G | Mean B | Pay Load Capacity (Samples) | Pay Load Capacity (%) |
|------------|--------|------|------|--------|--------|--------|----------------------------|-----------------------|
| RRR.bmp    | 11457.54 | 7.53 | 391.72 | 165.11 | 86.99  | 139.61 | 80000                      | 66.67                 |
| RRG.bmp    | 12932.16 | 7.01 | 377.76 | 165.11 | 86.99  | 125.65 | 80000                      | 66.67                 |
| RGR.bmp    | 15051.83 | 6.35 | 433.05 | 165.11 | 128.32 | 139.61 | 80000                      | 66.67                 |
| RGG.bmp    | 16526.45 | 5.94 | 419.09 | 165.11 | 128.32 | 125.65 | 80000                      | 66.67                 |
| GGG.bmp    | 23213.35 | 4.47 | 367.2  | 113.22 | 128.32 | 139.61 | 80000                      | 66.67                 |
| GGR.bmp    | 21738.73 | 4.75 | 381.16 | 113.22 | 128.32 | 139.61 | 80000                      | 66.67                 |
| GGG.bmp    | 18144.44 | 5.54 | 339.83 | 113.22 | 86.99  | 139.61 | 80000                      | 66.67                 |
| BBB.bmp    | 24771.1 | 4.19 | 259.76 | 132.04 | 127.71 |        | 80000                      | 66.67                 |
| BBR.bmp    | 20902.27 | 4.92 | 399.38 | 132.05 | 127.71 | 139.61 | 80000                      | 66.67                 |
| BRR.bmp    | 17167.9 | 5.78 | 358.65 | 132.04 | 86.99  | 139.61 | 80000                      | 66.67                 |
| BRG.bmp    | 18642.52 | 5.42 | 344.69 | 132.04 | 86.99  | 125.65 | 80000                      | 66.67                 |
| B GG.bmp   | 22236.82 | 4.66 | 386.02 | 132.04 | 128.32 | 125.65 | 80000                      | 66.67                 |
| GGB.bmp    | 25607.56 | 4.04 | 241.54 | 113.22 | 128.32 |        | 80000                      | 66.67                 |
| RRG.bmp    | 12932.16 | 7.01 | 377.76 | 165.11 | 86.99  | 125.65 | 80000                      | 66.67                 |
| RBB.bmp    | 15326.37 | 6.27 | 252.10 | 165.11 | 86.99  |        | 80000                      | 66.67                 |
| RBB.bmp    | 19060.73 | 5.32 | 292.82 | 165.11 | 127.71 |        | 80000                      | 66.67                 |

In the above data table the quantitative analysis of all 16 image shares are provided. In the above quantities Mean Square Error (MSE) & Peak Signal to Noise Ratio (PSNR) values are so very crucial because on the basis of them, the resultant cryptic image will be obtained. That resultant cryptic image file must have maximum MSE value against the fused image. As per above data table the image GGB.bmp has the maximum MSE value of 25607.56 against the fused image. Therefore this image is selected as the resultant cryptic image because it will be too difficult for the intruder or cracker to obtain the relevance between the resultant cryptic image and the fused image. Hence he/she can’t easily guess the set of images or image patterns or the process used for the password generation. Along with this the pay load analysis is also provided that narrates the total numbers of audio samples which can be replaced in the cryptic image, above maximum 8000 such samples of audio file can be replaced in the cryptic image with total capacity of 66.67% for the each share.

Following graph provides the details of Mean Square Error (MSE) obtained between all 16 images against the fused image.
In graph no 1, it can be observed that the MSE value of image GGN.bmp is highest in compare to all other images. Therefore it will be used as a share to generate our strong password string because even if intruder get this image still he/she cant decrypt it easily as this image appears very different from its source image. Due to the larger difference between the source image & the image GGB.bmp it will be very complicated for any intruder to decrypt the process & evaluate any clue for guessing our strong password key/string which is derived from the share GGB.bmp. therefore the current implemented system appears very robust & strong.

Comparative analysis of proposed method using some independent online tool:

The first online website used here is ‘passwordmeter.com’; this website provides the strength of the password depending on various parameters as shown in the following Screen shot (Screen shot #07).
In the above Screen shot the password string which is given as a input is generated using proposed method, in that the first obtained password was "$3?G\d,3@" this password string is given input to above website which results in 100% strength with very strong complexity level of the password. This password string has size of 10 letters only. The size of the password string can be further extendable (as per user’s requirement). There exist various parameters in the above website which evaluate the strength of the password string. All those parameters are also shown in above Screen shot.

4. Conclusion:

The current research work is dedicated to achieve access control & user authentication by Using Visual Cryptography. Here a mechanism is suggested by virtue of which the multi-share visual cryptography is implemented to generate the multiple shares of a secret image. Later one of the multiple shares is utilized to generate the strong password string/key to accomplish the task of preserving user authentication or access control.

References:

[1] James Kurose And Keith Ross “Computer Networks And Internet” Pearson Education Press, 05th Edition, 2019. Pp 713-715.

[2] Sadiq Almuairfi, Parakash Veeraraghavan And Naveen Chilamkurti, “IPAS: Implicit Password Authentication System”, 2011 IEEE International Conference On Advanced Information Networking And Applications(WAINA), Pp 430-435. ISBN 978-1-61284-829-7.

[3] Burnett, Mark (2016). Kleiman, Dave. Ed. “Perfect Passwords”, Rockland,Massachusetts: Syngress Publishing. P. 181. ISBN 1-59749-041-5.
[4] Ruchi Kumari, D.Krishna, V.Sridhar Reddy, “An Image Based Authentication Using Multi-Level Security System” DOI 10.4010/2013.230 ISSN-2321 -3361 © 2013 IJESC

[5] Forouzan And Mukhopadhyay “Cryptography & Network Security”, Mcgraw Hill India Press, 2010, Pp 1-3.

[6] Emin Islam Tathi, “Cracking More Password Hashes With Patterns”, IEEE Transactions On Information Forensics And Security, 2017.

[7] RICHARD SHAY, SARANGA KOMANDURI, ADAM L. DURITY, PHILLIP (SEYOUNG) HUH, MICHELLE L. MAZUREK, SEAN M. SEGREGTI, BLASE UR, LUJO BAUER, NICOLAS CHRISTIN, LORRIE FAITH CRANOR, “Designing Password Policies For Strength And Usability”, Vol 18, No. 4, ACM, May 2016.

[8] XAVIER DE CARN’E DE CARNAVALET And MOHAMMAD MANNAN, “A Large-Scale Evaluation Of High-Impact Password Strength Meters”, Vol 18, ACM, May 2018.

[9] Prof. Dr. Eng. Sattar B. Sadkhan, Dr. Baheeja K. AL-Shukur, Ali K. Mattar, “Survey Of Biometric Based Key Generation To Enhance Security Of Cryptosystems”, AIC-MITCSA, May 2016.

[10] Forouzan And Mukhopadhyay “Cryptography & Network Security”, Mcgraw Hill India Press, 2019, Pp 381-383.

[11] Alan Dalton, “Strong Password Generator”, 2014. [Online]. Available: Https://Strongpasswordgenerator.Com [Accessed: 09- Jan- 2016].

[12] Manik Lal Das, Ashutosh Saxena, And Ved P. Gulati, “A Dynamic ID-Based Remote User Authentication Scheme”, IEEE Transactions, Vol. 50, No. 2, MAY 2017.

[13] Jiang Huiping, “Strong Password Authentication Protocols”, IEEE International Conference On Distance Learning And Education, 2017.

[14] Masayuki Fukumitsu, Takashi Katoh, Bhed Bahadur Bista, Toyoo Takata “A Proposal Of An Associating Image-Based Password Creating Method And A Development Of A Password Creating Support System”, IEEE International Conference On Advanced Information Networking And Applications, 2016.

[15] Ilker Korkmaz, Mehmet Emin Dalkilic, “The Weak And The Strong Password Preferences: A Case Study On Turkish Users”, Copyright ACM, 2010.

[16] Sadiq Almuairfi, Parakash Veeraraghavan And Naveen Chilamkurti, “IPAS: Implicit Password Authentication System”, IEEE International Conference On Advanced Information Networking And Applications, 2011.

[17] Hung-Min Sun, Yao-Hsin Chen, And Yue-Hsun Lin, “Opass: A User Authentication Protocol Resistant To Password Stealing And Password Reuse Attacks”, Vol 7, IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, April 2017.

[18]Thomas Knoll, "Adobe Photoshop File Formats Specification" August2016,[Online]. Available:Https://Www.Adobe.Com/Devnet-Apps/Photoshop/Fileformatashtml.[Accessed:13-Dec-2016]

[19] Mamta Sharma And Sarika Khandelwal, "A Review On Multi Focal Image Fusion Techniques And Approaches" Vol. 5, Issue 9, September 2016.
[20] Xiangyu Wang, Yong Rui, Mohan Kankanhalli, “Up-Fusion: An Evolving Multimedia Fusion Method”, ACM Transactions. Multimedia Comput. Commun. Appl., Vol. 11, No. 1, August 2014.

[21] Yifeng Wang, Ping Zeng, Xuemei Luo, “Color Gamut Mapping Based On Image Fusion”, IEEE International Conference On Computer Science And Software Engineering, 2008.

[22] R. Guo, L. Zhang, M. Xing And J. Li, “Polarimetric SAR Image Fusion Using Nonnegative Matrix Factorisation And Improved-RGB Model”, Electronics Letters, Vol. 46 No. 20, 30th September 2010.

[23] Zhengguo Li, Jinghong Zheng, Zijian Zhu, And Shiqian Wu, “Selectively Detail-Enhanced Fusion Of Differently Exposed Images With Moving Objects”, IEEE Transactions On Image Processing, Vol. 23, No. 10, October 2017.

[24] Hailian Wang Xiaoguang Li Li Zhuo, “Exposure Fusion Via Textural And Color Transform”, IEEE Conference On Industrial Electronics And Applications, 2014.

[25] Huixian Wang, Wanshou Jiang, Chengqiang Lei, Shanlan Qin, And Jiaolong Wang, “A Robust Image Fusion Method Based On Local Spectral And Spatial Correlation”, IEEE Geoscience And Remote Sensing Letters, Vol. 11, No. 2, February 2014.

[26] Azmi Shawkat Abdulbaqi, Ahmed J. Obaid & Alyaa Hashem Mohammed (2021) ECG signals recruitment to implement a new technique for medical image encryption, Journal of Discrete Mathematical Sciences and Cryptography, DOI: 10.1080/09720529.2021.1884378.

[27] Manaa, Mehdi Ebady; Obaid, Ahmed J; Dosh, Mohammed Hussein, 2021. Unsupervised Approach for Email Spam Filtering using Data Mining, EAI Endorsed Transactions on Energy Web, DOI: 10.4108/eai.9-3-2021.168962.

[28] Oabid A.J., AlBermany S., Alkaam N.O. (2020) Enhancement in S-Box of BRADG Algorithm. In: Solanki V., Hoang M., Lu Z., Pattnaik P. (eds) Intelligent Computing in Engineering. Advances in Intelligent Systems and Computing, vol 1125. Springer, Singapore. https://doi.org/10.1007/978-981-15-2780-7_80.