Review Article

ACCENTS Transactions on Image Processing and Computer Vision, Vol 7(22)
ISSN (Online): 2455-4707
http://dx.doi.org/10.19101/TIPCV.2021.722002

A study and analysis of image security algorithms and the current challenges

Shubham Shashikant Patil[1*], Kailash Patidar[2], Gourav Saxena[3] and Narendra Sharma[3]

M.Tech Student, Computer Science and Engineering, SSSIST, Sehore, Madhya Pradesh, India[1]

Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[2]

Assistant Professor, Department of Computer Science, School of Engineering, Sri Satya Sai University of Technology & Medical Sciences, Sehore, Madhya Pradesh, India[3]

Received: 03-January-2021; Revised: 20-February-2021; Accepted: 23-February-2021

Abstract

In any era, communication is very important. In today's era effective data communication is important in all the fields. Here effectiveness was used in terms of secure communication. So, communication in the way that it is secure from any unauthorized access is important. In this paper a study and analysis were performed in the direction of image data security. This paper explores the current trends in the direction of image data security. It covers methods for image data security, tools and techniques, current challenges along with suggestive measures. It also explores the mitigating ways and directions to achieve high level image data security in the means of data communication. Cryptography and steganography methods were also being discussed, so that better methods can be selected for achieving high level data security.

Keywords

Image data security, Unauthorized access, Cryptography, Steganography.

1.Introduction

In the current communication trend, data transmission through different media is increasing day by day [1]. The main data used in the communication are text, images and video. The wide use of data sending and receiving in terms of different pictures increases the demand of image data security. There are different dimensions in the image security research work. There is a lot of research work is going on including different dimensions and aspects [2–10]. These aspects include cryptography and steganography techniques along with other mechanism for security breach detection also [11–15].

Security mechanism in general handled by cryptography and steganography algorithms [16–21]. In general, the mechanism of encryption and decryption of data is handled through cryptography algorithms [22, 23]. The data hiding mechanism has been adopted in case steganography [24]. .

This paper covers the study, analysis and discussion in case of image data security. *Figure 1* shows the need of data security. It clearly emphasizes the need of data security in terms of breach control, access control and network security. Activity monitoring, may be performed based on these factors [22–25]. *Figure 2* shows the role of data integrity. It consists of constraints, data filtration, attributes, threshold and combined actuation. *Figure 3* shows the different layers in achieving image security

So, this paper mainly shows the insights and the current trends in the image data security for the exploration of the need and challenges.

The objectives of this paper are as under:

1. To explore the image data security algorithms, especially in terms of data communication.
2. To explore the challenges and gaps in the same direction.
3. To explore the method's applicability and parametric study.
4. To analyse the related results for the impact analysis.

*Author for correspondence

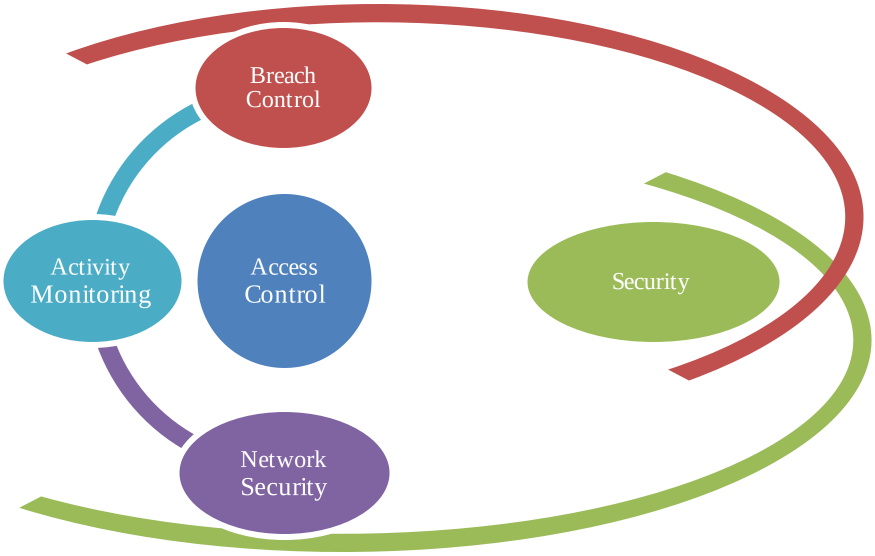

Figure 1 Need of image data security

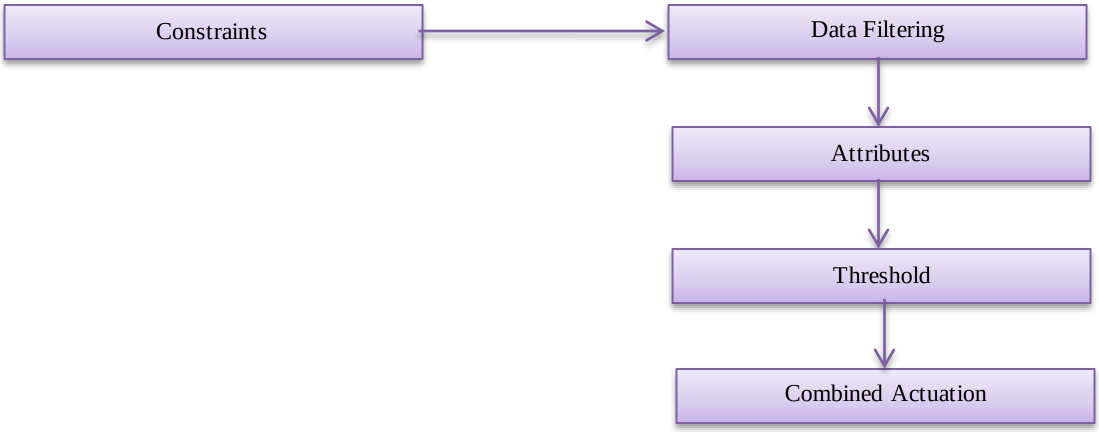

Figure 2 Role of data integrity

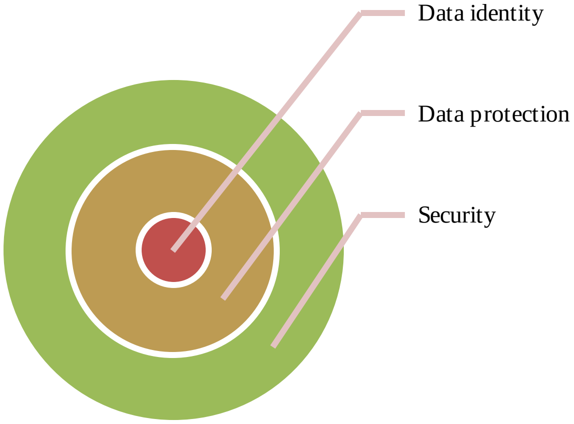

Figure 3 Different layers in achieving image security

2.Literature survey

In 2020, Kushnir et al. [26] discussed the crucial aspects of security through chaotic encryption. The image encryption technique has been proposed by using two chaotic mappings. They used fuzzy logic for the same. Statistical analysis was performed based on the histogram, entropy and correlation coefficient computation.

In 2020, Han et al. [27] proposed an encryption algorithm based on medical domain. The main procedure is oriented through the Hermite chaotic neural network. Training was performed based on Hermite chaotic neural network. Experimentation was performed on medical image. The results indicate the improved performance in terms of key space and sensitivity.

In 2020, Kaur and Jindal [28] analyzed and explored the image authentication techniques. Singular value decomposition (SVD) was used along with the extraction. Important features of images were extracted based on this QR code.

In 2020, Abdulrahman and Varol [29] discussed and analyzed the importance of image segmentation. They have processed their approach based on color density. It has been used for segment evaluation. Their approach was used in medical, cultural and industrial fields. They reviewed image segmentation, threshold functions and different aspects apply for images.

In 2020, Zhang et al. [30] discussed and analyzed the properties of unpredictability. It is used in terms of initial values and parameters and chaotic systems. They proposed a 2D logistic scheme for the coupling modulation model. It is based on chaotic ring transformation. Diffusion operation has been performed on pixel values. It is found to be more secure and strong.

In 2020, Abdallah [31] discussed about computed tomography. They used water-based segmentation. It is used for the detection of the margin's tissues within the images. Contrast augmentation and segmentation were used for the lesion detection. It has been endorsed by the achievability and efficiency. It is found to be effective in the smaller lesion detection.

In 2020, Yadahalli et al. [32] discussed about the steganography techniques. It is employed based on the confidential messages in terms of data transmission. They have used least significant bit method along with the discrete wavelet transform method. Their results indicate the effectiveness of the approach.

In 2020, Luo and Zhu [33] discussed and analyzed the deep learning model. They used x-ray pictures for the experiment. They used data augmentation method. It is found to be more effective. It is found to that more complex backbone can be found to be more sensitive.

In 2020, Kukharska et al. [34] discussed about the stenographic data transformation. Their proposed approach provides the facility of embedding secret information along with the changes of images between its pixel values. The Arnold's transformation was used for the rearrangement. The results indicate that the visual image quality was unchanged for the hidden information detection.

In 2020, Kumar et al. [35] discussed about image segmentation. Their main aim is to identify the nucleus of white blood cells. They evaluated the efficiency based on the edge detection algorithm (log & Canny) methods, k-means algorithm, linear transformed image and color-based technique. They provided the comparative analysis of the same.
Their results indicate that the k-means based segmentation is found to be suitable.

In 2020, Arpac and Kurt [36] discussed about different GUI tools. It has been designed and implemented for the cryptographic applications. Their tool is efficient to improve the security of the encryption process. It includes security tests for different domains like noise attack, key sensitivity and differential attacks.

3.Discussion and comparative analysis

A different security mechanism has been discussed and analyzed along with the computational capability and current progress in this field. Based on the analysis and discussion, it is clear that there is high demand of security in almost every area of communication (*Table 1*).

Table 1 Method and result analysis of some selected study

S.NO	Reference	Method	Approach	Results achieved
1	[37]	Cryptographic solutions	They have suggested that the cloud computing cryptography may be helpful in safe and secure cloud computing design. It incorporates a gathering of heedless virtualized animated adaptable and oversaw assets like processing control extra room stage and administrations. They have also applied statistics coding for the virtualization mechanism. They have also discussed the safety weaknesses of cloud computing. They have also suggested that the victimization biometric coding also enhance the security.	Security enhancement views has been presented and discussed.
2	[38]	Security enhancement in storage area network	They have suggested that the storage area network (SAN) has the capability of distributed storage for the data aggregation from several private nodes into a centralized secure place. A SAN security structure should be created and planned. Their research work highlighted the security vulnerabilities for different attacks. It is based on SAN protocols for the comparison.	Their aim is to enhance the security system.
3	[39]	Profiling and preventing security attacks	They have proposed a model called "profiling furthermore, averting security assaults", to recognize furthermore, avert the referred to attacks just as the obscure assaults before getting to the cloud administrations/assets. They have suggested different new security factors which are keystroke dynamic. Their approach is the combination of machine learning algorithm in order to profile and predict security attacks.	Different security and srvices parameters have been discussed with the case study.
4	[40]	Communication over cloud computing	They have discussed cloud computing model with the on-demand access to the shared pool configurable computing resources. In distributed computing, IT related capacities are given as administrations, accessible without requiring a profound information of the basic advances, additionally, with unimportant organizational effort. The security issue ends up being progressively intricate under the haze model as new estimations have gone into the issue extensively identified with the model design, multi-tenure, flexibility, and layers reliance stack.	They have reviewed and discussed different security issues.
5	[41]	Enhanced visual cryptography	They have presented two schemes to secretly share images enhanced visual cryptographic scheme and visual cryptographic scheme. It utilizes the concept of keys to secure information. It is based on visual cryptography.	It is found to be an efficient and secure mechanism.

4.Problem identification

This study suggests the following observations:

1. There is the need of image data security in different communication domains with the ease of proper communication capabilities.
2. There is the need of hybrid security with the data sensitivity estimation for providing an efficient security framework.
3. There is the need of different algorithms based on the data type and the nature of the data.
4. There is the need of parametric evaluation and data ranking so that different level of security sensitivity can be applied.

5. Conclusion

This paper mainly discussed and analyze the methods in the image data security field. It covers the methods, approach, data variety and approach applicability. It explores the data reliability, image security aspects and protection mechanism. Different methods have been discussed and analyzed with the current trends. It also explores the gaps in terms of different security and computational aspects. In future a hybrid framework can be designed considering security and image sensitivity.

Acknowledgment

None.

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] Kocarev L. Chaos-based cryptography: a brief overview. IEEE Circuits and Systems Magazine. 2001; 1(3):6-21.

[2] Sasubilli SM, Dubey AK, Kumar A. Hybrid security analysis based on intelligent adaptive learning in Big Data. In International Conference on Advances in Computing and Communication Engineering 2020 (pp. 1-5). IEEE.

[3] Qiu J, Wang P. An image encryption and authentication scheme. In International Conference on Computational Intelligence and Security 2011 (pp. 784-787). IEEE.

[4] Sasubilli SM, Dubey AK, Kumar A. A computational and analytical approach for cloud computing security with user data management. In International Conference on Advances in Computing and Communication Engineering 2020 (pp. 1-5). IEEE.

[5] Hu G, Feng Z, Wang L. Analysis of a type of digital chaotic cryptosystem. In International Symposium on Circuits and Systems. Proceedings 2002 (Vol. 3, pp. III-III). IEEE.

[6] Boiko J, Kovtun I, Petrashchuk S. Productivity of telecommunication systems with modified signal-code constructions. In International Scientific-Practical Conference Problems of Infocommunications. Science and Technology 2017 (pp. 173-178). IEEE.

[7] Millérioux G, Amigó JM, Daafouz J. A connection between chaotic and conventional cryptography. IEEE Transactions on Circuits and Systems I: Regular Papers. 2008; 55(6):1695-703.

[8] Zahan A, Hossain MS, Rahman Z, Shezan SK. Smart home IoT use case with elliptic curve based digital signature: an evaluation on security and performance analysis. International Journal of Advanced Technology and Engineering Exploration. 2020;7(62):11-9.

[9] Ni Z, Shi YQ, Ansari N, Su W. Reversible data hiding. IEEE Transactions on Circuits and Systems for Video Technology. 2006;16(3):354-62.

[10] Nazmudeen NH, Farsana FJ. Satellite image security improvement by combining DWT-DCT watermarking and AES encryption. International Journal of Advanced Computer Research. 2014;4(2):645-52.

[11] Seethalakshmi AV, Hemachitra HS. Complex type seed variety identification and recognition using optimized image processing techniques. ACCENTS Transactions on Image Processing and Computer Vision. 2020; 6 (19): 23-31.

[12] Gladwin SJ, Gowthami PL. Combined cryptography and steganography for enhanced security in suboptimal images. In International Conference on Artificial Intelligence and Signal Processing 2020 (pp. 1-5). IEEE.

[13] Al-Kadei FH, Mardan HA, Minas NA. Speed up image encryption by using RSA algorithm. In International Conference on Advanced Computing and Communication Systems 2020 (pp. 1302-1307). IEEE.

[14] Duan X, Guo D, Liu N, Li B, Gou M, Qin C. A new high capacity image steganography method combined with image elliptic curve cryptography and deep neural network. IEEE Access. 2020; 8:25777-88.

[15] Dubey AK, Dubey AK, Namdev M, Shrivastava SS. Cloud-user security based on RSA and MD5 algorithm for resource attestation and sharing in java environment. In CSI international conference on software engineering 2012 (pp. 1-8). IEEE.

[16] Sharma V, Shukla M, Srivastava S, Mandal R. Generative network based image encryption. In International Conference on Intelligent Computing and Control Systems 2020 (pp. 1-5). IEEE.

[17] Abhinav A, Manikandan VM, Bini AA. An improved reversible data hiding on encrypted images by selective pixel flipping technique. In international conference on devices, circuits and systems 2020 (pp. 294-8). IEEE.

[18] Santos TA, Magalhães EP, Basílio NP, Nepomuceno EG, Karimov TI, Butusov DN. Improving chaotic image encryption using maps with small Lyapunov exponents. In Moscow workshop on electronic and networking technologies 2020 (pp. 1-4). IEEE.

[19] Hu D, Zheng Y, Zhang H, Sun S, Xie F, Shi J, Jiang Z. Informative retrieval framework for histopathology whole slides images based on deep hashing network. In international symposium on biomedical imaging 2020 (pp. 244-8). IEEE.

[20] Wahid SD, Buja AG, Jono MH, Aziz AA. Assessing the influential factors of cybersecurity awareness in Malaysia during the pandemic outbreak: a structural equation modeling. International Journal of Advanced Technology and Engineering Exploration. 2021; 8 (74): 73-81.

[21] Kalaichelvi T, Apuroop P. Image steganography method to achieve confidentiality using CAPTCHA for authentication. In international conference on communication and electronics systems 2020 (pp. 495-499). IEEE.

[22] Ye H, Huang S, Liu W. Research on image scrambling method based on combination of Arnold transform and exclusive-or operation. In information technology, networking, electronic and automation control conference 2020 (Vol. 1, pp. 151-154). IEEE.

[23] Srivastava M, Siddiqui J, Ali MA. Local binary pattern based technique for content based image copy detection. In international conference on power electronics & IoT applications in renewable energy and its control 2020 (pp. 374-377). IEEE.

[24] Samvatsar M, Kanungo P. An analytical review and analysis for the data control and security in cloud computing. International Journal of Advanced Technology and Engineering Exploration. 2020; 7(73):241.

[25] Pramanik S, Bandyopadhyay SK, Ghosh R. Signature image hiding in color image using steganography and

cryptography based on digital signature concepts. In international conference on innovative mechanisms for industry applications 2020 (pp. 665-9). IEEE.

[26] Kushnir M, Kosovan H, Kroialo P, Komarnytskyy A. Encryption of the images on the basis of two chaotic systems with the use of fuzzy logic. In international conference on advanced trends in radioelectronics, telecommunications and computer engineering 2020 (pp. 610-3). IEEE.

[27] Han B, Jia Y, Huang G, Cai L. A medical image encryption algorithm based on Hermite chaotic neural network. In information technology, networking, electronic and automation control conference 2020 (Vol. 1, pp. 2644-8). IEEE.

[28] Kaur S, Jindal A. Singular value decomposition (SVD) based image tamper detection scheme. In international conference on inventive computation technologies 2020 (pp. 695-9). IEEE.

[29] Abdulrahman A, Varol S. A review of image segmentation using MATLAB environment. In international symposium on digital forensics and security 2020 (pp. 1-5). IEEE.

[30] Zhang H, Zhu J, Zhao S, He O, Zhong X, Liu J. A new image encryption algorithm based on 2D-LSIMM chaotic map. In international conference on advanced computational intelligence 2020 (pp. 326-333). IEEE.

[31] Abdallah Y. Segmentation of brain stroke lesions using marker-based algorithms in CT images. In international conference on computer applications & information security 2020 (pp. 1-4). IEEE.

[32] Yadahalli SS, Rege S, Sonkusare R. Implementation and analysis of image steganography using least significant bit and discrete wavelet transform techniques. In international conference on communication and electronics systems 2020 (pp. 1325-30). IEEE.

[33] Luo Y, Zhu L. Research on data augmentation for object detection based on x-ray security inspection picture. In international conference on advances in electrical engineering and computer applications 2020 (pp. 219-22). IEEE.

[34] Kukharska N, Lagun A, Polotai O. The steganographic approach to data protection using Arnold algorithm and the pixel-value differencing method. In international conference on data stream mining & processing 2020 (pp. 174-177). IEEE.

[35] Kumar PR, Sarkar A, Mohanty SN, Kumar PP. Segmentation of white blood cells using image segmentation algorithms. In international conference on computing, communication and security 2020 (pp. 1-4). IEEE.

[36] Arpac B, Kurt E. An innovative tool for the chaotic image encryption, decryption and security tests. In international conference on electrical, communication, and computer engineering 2020 (pp. 1-8). IEEE.

[37] Abedin ZU, Guan Z, Arif AU, Anwar U. An advance cryptographic solutions in cloud computing security. In international conference on computing, mathematics and engineering technologies 2019 (pp. 1-6). IEEE.

[38] Chukry S, Sbeyti H. Security enhancement in storage area network. In international symposium on digital forensics and security 2019 (pp. 1-5). IEEE.

[39] Eddermoug N, Sadik M, Sabir E, Mansour A, Azmi M. PPSA: profiling and preventing security attacks in cloud computing. In international wireless communications & mobile computing conference 2019 (pp. 415-21). IEEE.

[40] Tanash RM, Ala'F K, Darabkh KA. Communication over cloud computing: a security survey. In international convention on information and communication technology, electronics and microelectronics 2019 (pp. 496-501). IEEE.

[41] Tripathi J, Saini A. Enhanced visual cryptography: an augmented model for image security. Procedia Computer Science. 2020; 167:323-33.

Shubham Patil received the B.E degree in Information Technology from North Maharashtra University, Jalgaon, Maharashtra in 2013. He is Currently pursuing M.Tech from SSSUTMS, Sehore, MP.

Email: meet2shub@gmail.com