DOI:

Image Encryption Using Different Cryptographic Algorithms : A Survey Paper

Fr. Jins Sebastian Arackaparampil, Manu Tom Sebastian, Minnu Elsa Baby, Niya Mary Viby
Department of Electronics and Communication Engineering
Amal Jyothi College of Engineering
Kanjirappally, India
jinsarackaparampil@amaljyothi.ac.in,
manutomsebastian@gmail.com,
minnuelsababy@gmail.com, niyamviby2000@gmail.com,

Dr. Kumar S.N
Department of Electrical and Electronics Engineering
Amal Jyothi College of Engineering
Kanjirappally, India
snkumar@amaljyothi.ac.in

***Abstract*——Nowadays while transferring and receiving the data like images, messages and other information, certain encryption methods are used to increase the security of that data. By using the encryption method, we can prevent the loss of data or can maintain the confidentiality or integrity of the data. In this paper we will study about the survey that we conducted about the encryption of image using different cryptographic algorithms.**

Keywords—Image Encryption, Cryptographic Algorithm, Security.

I. Introduction

Over the years, the internet has evolved it's way of sharing information, organizing the flow of things and how we all connect with others all over the world. Due to it's rapid growth and the large influence on all individuals, the internet has become a vital part in our day to day life. Internet helps us to share information or important data to others all over the world without any physical contact. But the sharing of confidential data virtually will be facing issues like attacks, data breach, data loss and data modifications which will cause a huge loss for the sender and receiver. Therefore, it is important to add some security measures to our data that is shared to prevent such cyber-attacks. So, in order to prevent these attacks certain cryptographic encryption algorithms are used and by doing this we can ensure the safety and integrity of the data that we share.

Encryption is a process that is used to code the data or hide the original data and then convert this data into another form so that unauthorized users cannot access the original data. One such data that need this encryption method are the images that we share. Some images contain confidential information based on the fields that they are used. Health care sector is one such field where they have medical images or electronic health records of a patient. These images contain all the information's about the disease or personal information of the patients. The rapid growth of internet over the years has enabled the health care sector to share these medical images to authorized users and they can also store this data in a virtual memory or in their online applications. And this approach has been increased due to the appearance of the contagious disease called COVID-19. Due to this high dependent usage of internet for sharing or storing the images or the data, there is a high chance for data breaches and the misusage of these data to happen in the future. Therefore, it is very important to encrypt the data using a cryptographic algorithm to avoid the cyber-attacks and to protect the confidentiality of the image. By using this method, the image can be converted into an unrecognizable form which makes it very difficult for the unauthorized users to understand or to get information from the original image. In order to convert the image into an unrecognized form we collect all the parameters and values by performing the image processing method.

Image processing is method of converting an image into a digital form so that some operations can be performed in order to get some useful information from it. The encryption process can be performed on the digital data of the image that is converted by the image processing. That is the digital data can be manipulated according to the methods of cryptographic algorithm to get the encrypted image. These methods include pixel rotation, shifting of row and column of the matrix form of the image, etc. After performing the preferred cryptographic algorithm, we can say that the image can be protected from all the cyber-attacks and we can maintain the confidentiality and integrity of the information that we share through the internet

In this paper we will be seeing about the survey that we have conducted in order to find a better cryptographic algorithm for the encryption of image data. Here we will see different cryptographic algorithm used by others for the image encryption and we will see the methods that they have used and what they all have achieved by performing those cryptographic algorithms.

II. Related Works

Here we will discuss about some of the related works with respect to the image encryption process. [1] Networked 3D printers are an emerging trend and pose security challenges in the manufacturing area. Since, it needs to be addressed about the safety and security of the printing process. Prior to that work on 3D printer attack has experimented that an attacker can create defective parts by broadening CAD files. As we are aware about the fact that these deployments are increasing, should be vigilant about it. However, it was suggested by Matthew Mc Cormack for identifying if a 3D printer is susceptible to any danger. The method used is C3PO .As this tool can be used for identifying the error and also analyse about the network disposition. [2] 3D printing has become a major technology in many sectors and playing a vital role. Yet, the object can be printed both online and physically it raises remarkable copyright infringement difficulties. It was discussed by Jong-Uk Hou about the various technologies like cryptography, digital rights management (DRM), digital watermarking and fingerprinting. These are conventional technologies used. Provides better security. [3] With the advancement of 3D printing technology, it is important that the 3D printing models are encrypted before being transmitted and used. Giao N. Pham proposed a novel perceptual algorithm for the 3D models. This algorithm uses three control points, an interpolating factor. A secret key is used to encrypt the control points. Moreover, by using inverse interpolation and geometric distortion the encrypted properties of the spline curve area. [4] Nowadays, conventional supply chains are replaced by value added networks. In this research work the key technology used is digital rights management (DRM). The study was conducted by Martin Holland. This was implemented by using blockchain. The concept was demonstrated as a licensor and a licensee uses a secret key that offers a secure transition. For e.g. The barcode labelled on a product is secured with this method. This is accessible only for the copyright holder. The holder provides patent to the receiver. This comes under copyright law. [5] As it was analysed that the conventional methods provide protection but they are not that much effective. Jong Uk-Hou proposed a robust and blind watermark scheme. This method not only provides protection when the content is shared digitally but also when they are converted to analogy. So it was implemented by embedding watermark information into 3D model and detects the information that is embedded. The z-axis of the model is aligned with printing direction to achieve blind detection. This is done during the printing process. [6] The method was proposed by Giao N. Pham. The proposed algorithm was selective encryption for 3D printing models. The models were in the frequency domain of the discrete cosine transform (DCT). The method was implemented to prevent illegal copying , access in the secured storage. In the current scenario 3D printing uses 3D triangle meshes to print the objects. As it analyses the entropy of the 3D mesh by pointing out that if the entropy is high , security will be high. [7] Here the paper features about an efficient 3D data masking method purely based on watermarking algorithm. It provides high masking capacity. It was proposed by Manik Amma Malipatil. An efficient watermarking method for 3D mesh models. The outcome of this method is that a better SNR performance can be attained . Moreover , the recovered mesh is invisible to naked eye , because a higher quality is attained. [8] A chaos-based encryption algorithm is used. In that scheme Arnold Transform is taken. The algorithm was proposed by Benson Raj. Here it is seen that the use of this map is to encrypt the 3D model using shuffling and substitution. By implementing this method leads to more chaos and better encryption. It provides better security than other methods. [9] Here in the paper it gives a new direction to technical steganography. This concept was proposed by Alexandr Kuzentsov. It gives a detailed study about information data converted to digital 3D model placed inside a container product. After the printing process, the extracted object contains information data that cannot be deleted or distorted. [10] The algorithm used here is discrete cosine transform (DCT). It was put forward by Zhang Changao. It was done through k-means clustering method. The result shows that by using the above algorithm it can effectively resist geometric attacks and has good robustness. [11] Padmanabhan proposed a new technique of encrypting 3D model information using 2D images. 3D data is stored in 2D images for greater freedom in encryption without losses. This technique enhances cybersecurity for 3D models. It can be easily converted back to 3D model at the user end. [12] Ch. Ratna Babu proposed a novel method of Visual Cryptography for halftone images. Pseudo-randomization and pixel reversal-based visual information concealment are also suggested. Here the decrypted image and original image are of same size. This technique increases security due to randomness. The recommended future work involves pixel enlargement and contrast enhancement in the final secret image as well as extending the technique to colour images. [13] Hongjun Liu proposed a new method, 3D improved coupling quadratic map (3D-ICQM) with sine function. Then its randomness is evaluated by TestU01 with different gains. 3D-ICQM based picture encryption method was developed that includes round key expansion and cypher feedback. Experimental findings and statistical analysis demonstrated that the suggested scheme outperforms several current algorithms in terms of efficacy and viability. [14] Misung Cho proposed fingerprinting and encryption method called as Joint Fingerprinting and Decryption (JFD) scheme of 3D data. The suggested JFD approach is built on a novel partial encryption of 3D data that encrypts only a small portion of the plaintext to reduce processing. As a result of partial decryption, each fingerprint has a distinctive imprint. By comparing the mark in the retrieved copy with a list of reference marks, fingerprints are detected. [15] P. Mohan Kumar proposed a brand-new multi-layered embedding approach in order to increase the hiding capability. This steganography method uses a cutting-

DOI:

edge embedding methodology to conceal encoded information in the vertices of 3D polygon models. By adhering to the low distortion and security fundamental requirements for steganography on 3D models, this unique approach can offer a significantly larger hiding capacity than other cutting-edge approaches. This method may steganographically conceal far larger bit rates/vertex than any prior state-of-the-art techniques for 3D polygon models. [16] To ensure the safety of data transmitted from all the cyberattacks Dang, P. P. proposed an image encryption method which focuses on the image encryption by using IDEA algorithm. Here compression algorithm is also included in the encryption algorithm. And it also includes the implementation in software and implementation in hardware for system architecture of IDEA algorithm for encryption of image that is based on the Field Programmable Gate Array (FPGA) technology. Using this type of encryption scheme a lot of cyber-attacks can be prevented. [17] Kuo, C. J. proposed a method where the encryption of the image is achieved by changing the original image's phase spectra. In this encryption technique the phase spectra of an input image is added with a pseudo noise's binary phase. By doing this the input image's binary spectra are changed randomly which makes the encrypted image unrecognizable. Therefore, many of the attacks can be prevented because there are many ways to alter the phase spectra of the input image. This method of encryption is similar to the cryptographic system using a private key. The image encryption technique used here is suitable for progressive transmission. The main advantage of this encryption technique is that it has the ability to stop the transmission of image at any time and can reconstruct a meaningful image. [18] Bourbakis, N. proposedIn this paper the image data is encrypted using scan patterns. Here the 2D data array of the image is taken and it is then converted into a 1D list which ranges between a specific interval. The encryption is performed on the 2D image data using a group of scanning patterns. That is a transposition transformation is done on the input data. Thus, after applying the scanning patterns the image array in 2D is transformed into 1D. Here the encryption algorithm is obtained from SCAN language implementation algorithm. The SCAN language contains one parallel and one sequential encryption algorithms. This encryption type can be used for the image data protection that is stored in the sequential files, the digital images encryption during transmission, as well as for encryption for numerical data in 2D. [19] Kotulski, Z. proposed a method where utilization of the unpredictable property of discrete chaotic systems is used as a way of constructing cryptosystems. The main feature of chaos is that the trajectories can be generated by simple deterministic nonlinear systems, which are random. Its main property is that there is the systems extreme sensitivity to initial conditions. Here the discrete chaotic cryptosystem (DCC) is based on the inverse and forward iterations of a discrete chaotic map (during the encryption and decryption). After using DCC algorithm, the encrypted messages are spread all over the ciphertexts whole space. By using the specific key value, the original data can be retrieved. This method proves to be more secure and efficient. It is less vulnerable to all the attacks. [20] Fridrich, J. prosed a technique which describes how the image encryption can be performed using two dimensional chaotic maps. This method can be applied when there is large amount of data that needs to be protected, such as digital images. Here a symmetric block encryption method which is based on 2D chaotic map is performed. Some of its main features are the large size of the block, variable key length and higher encryption rate. After the encryption process is performed it is seen in the result that the cipher seems to have better diffusion properties with respect to both the plain-text and the key. Therefore, the security level of this method is high. This method can be used in a wide variety of fields and can be modified to improve and add other features.

III. Conclusion

After conducting the survey on many related works having different cryptographic algorithms for image encryption, we can see that each methods have it's on advantages and disadvantages. Each of the methods have there on properties and advantages which make them stand out or makes them unique when compared to the other methods. Therefore, we can say that when choosing a specific algorithm, we have to consider the field that we are applying the algorithm, the advantages that we need and the disadvantages that we need to avoid for that particular field. All the cryptographic algorithms that we have seen here have proved that they did a better job in securing the image data, prevented all the cyber-attacks and the entry of all unauthorized users and maintained the confidentiality and integrity of the data that is shared or stored.

Acknowledgment

This work was executed with the support and guidance of Fr. Jins Sebastian Arackaparambil, Assistant Professor and Dr. Kumar S.N, Assistant Professor of Amal Jyothi Collage of Engineering.

References

[1] M, Chandrasekaran S, Liu G, Yu T, Wolf SD, Sekar V. "security analysis of networked 3d printers". In2020 IEEE Security and Privacy Workshops (SPW) 2020 May 21 (pp. 118-125). IEEE.

[2] Hou JU, Kim D, Ahn WH, Lee HK. "Copyright protections of digital content in the age of 3d printer: Emerging issues and survey". IEEE Access. 2018 Aug 9;6:44082-93.

[3] Pham GN, Lee SH, Kwon KR. "Interpolating spline curve-based Perceptual Encryption for 3D printing models". Applied Sciences. 2018 Feb 5;8(2):242.

[4] Holland M, Stjepandić J, Nigischer C. "Intellectual property protection of 3D print supply chain with blockchain technology". In2018 IEEE International conference on engineering, technology and innovation (ICE/ITMC) 2018 Jun 17 (pp. 1-8). IEEE.

[5] Hou JU, Kim DG, Lee HK. "Blind 3D mesh watermarking for 3D printed model by analyzing layering artifact". IEEE Transactions on Information Forensics and Security. 2017 Jun 21;12(11):2712-25.

DOI:

[6] Pham GN, Park JH, Kwon OH, Song HJ, Lee SH, Moon KS, Kim ST, Cho YR, Kwon KR. “Selective Encryption for 3D Printing Model in DCT Domain”. In2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN) 2018 Jul 3 (pp. 398-400). IEEE.

[7] Malipatil M, Shubhangi DC. “An efficient 3D Watermarking algorithm for 3D mesh models”. In2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC) 2020 Oct 7 (pp. 1-5). IEEE.

[8] Raj B, Jani Anbarasi L, Narendra M, Subashini VJ. “A new transformation of 3D models using chaotic encryption based on arnold cat map”. InAdvances in Internet, Data and Web Technologies: The 7th International Conference on Emerging Internet, Data and Web Technologies (EIDWT-2019) 2019 (pp. 322-332). Springer International Publishing.

[9] Kuznetsov A, Stefanovych O, Gorbenko Y, Smirnov O, Krasnobaev V, Kuznetsova K. “Information hiding using 3D-printing technology”. In2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS) 2019 Sep 18 (Vol. 2, pp. 701-706). IEEE.

[10] Changhao Z, Hu L, Hao L, Peng S. “Research on Information Encryption and Hiding Technology of 3D Point Cloud Data Model”. In2020 International Conference on Computer Science and Management Technology (ICCSMT) 2020 Nov 20 (pp. 54-58). IEEE.

[11] Padmanabhan A, Zhang J. “Cybersecurity risks and mitigation strategies in additive manufacturing. Progress in Additive Manufacturing”. 2018 Jun;3:87-93.

[12] Babu CR, Sridhar M, Babu BR. “Information hiding in gray scale images using pseudo-randomized visual cryptography algorithm for visual information security”. In2013 International Conference on Information Systems and Computer Networks 2013 Mar 9 (pp. 195-199). IEEE.

[13] Liu H, Kadir A, Xu C. “Color image encryption with cipher feedback and coupling chaotic map”. International Journal of Bifurcation and Chaos. 2020 Sep 30;30(12):2050173.

[14] Cho M, Kim S, Sung M, On G. “3d fingerprinting and encryption principle for collaboration”. In2006 Second International Conference on Automated Production of Cross Media Content for Multi-Channel Distribution (AXMEDIS'06) 2006 Dec 13 (pp. 121-127). IEEE.

[15] Kumar PM, Shunmuganathan KL. “A Multilayered architecture for hiding executable files in 3D images”. Indian Journal of Science & Technology. 2010 Apr;3.

[16] Dang PP, Chau PM. “Implementation of the IDEA algorithm for image encryption”. InMathematics and Applications of Data/Image Coding, Compression, and Encryption III 2000 Nov 17 (Vol. 4122, pp. 1-9). SPIE.

[17] Kuo CJ. “Novel image encryption technique and its application in progressive transmission”. Journal of Electronic Imaging. 1993 Oct;2(4):345-51.

[18] Bourbakis N, Alexopoulos C. “Picture data encryption using scan patterns”. Pattern Recognition. 1992 Jun 1;25(6):567-81.

[19] Kotulski Z, Szczepański J, Górski K, Paszkiewicz A, Zugaj A. “Application of discrete chaotic dynamical systems in cryptography—DCC method”. International Journal of Bifurcation and Chaos. 1999 Jun;9(06):1121-35.

[20] Fridrich J. “Image encryption based on chaotic maps”. In1997 IEEE international conference on systems, man, and cybernetics. Computational cybernetics and simulation 1997 Oct 12 (Vol. 2, pp. 1105-1110). IEEE.