IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 10, October 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910022 |

A Technical Survey on Image Encryption using Block Transformation and Carrier Image

P.Boobalan[1], Mr.K.Gunasekar[2]

PG Scholar, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India[1]

Head of Department, Department of Computer Science and Engineering, Nandha Engineering College (Autonomous), Erode, Tamilnadu, India[2]

ABSTRACT: Educational The Information security has become more important with the progress in the exchange of data and various encryption systems to encrypt and decrypt image. Most of the encryption algorithm available is generally used for text data and not suitable for multimedia data. This project aims to design and develop new methods for image encryption using Block transformation process and Random number generation which ensures high level of security. In Block transformation process, the blocks of the image considered as a matrix are rearranged with respect to SCAN pattern which results in an image entirely different from that of the original image.

KEYWORDS: Encryption, Block transformation process, Random number generation.

I. INTRODUCTION

Currently, Encryption is used to securely transmit data in open networks. Each type of data has its own features, therefore different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images. In this paper, we introduce a block-based transformation algorithm based on the combination of image transformation and a well-known encryption and decryption algorithm called Blowfish. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm presented here, and then the transformed image was encrypted using the Blowfish algorithm. The results showed that the correlation between image elements was significantly decreased by using the proposed technique. The results also show that increasing the number of blocks by using smaller block sizes resulted in a lower correlation and higher entropy.

1. Image Encryption:

Image encryption is a useful technique of image content protection. It converts images into noise- like encrypted images by disrupting pixel positions or changing pixel values. In recent years, researchers have developed many useful image encryption algorithms.

Block Transformation

Transform coding compresses image data by representing the original signal with a small number of transform coefficients. It exploits the fact that for typical images a large amount of signal energy is concentrated in a small number of coefficients.

The term is much more commonly used in digital media and digital signal processing. The most widely used transform coding technique in this regard is the discrete cosine transform (DCT), proposed by Nasir Ahmed in 1972, and presented by Ahmed with T. Natarajan and K. R. Rao in 1974. This DCT, in the context of the family of discrete cosine transforms, is the DCT-II. It is the basis for the common JPEG image compression standard, which examines small blocks of the image and transforms them to the frequency domain for more efficient quantization (lossy) and data compression. In video coding, the H.26x and MPEG standards modify this DCT image compression technique across frames in a motion image using motion compensation, further reducing the size compared to a series of JPEGs.

In audio coding, MPEG audio compression analyzes the transformed data according to a psychoacoustic model that describes the human ear's sensitivity to parts of the signal, similar to the TV model. MP3 uses a hybrid coding algorithm, combining the modified discrete cosine transform (MDCT) and fast Fourier transform

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910022 |

(FFT). It was succeeded by Advanced Audio Coding (AAC), which uses a pure MDCT algorithm to significantly improve compression efficiency.
The basic process of digitizing an analog signal is a kind of transform coding that uses sampling in one or more domains as its transform.

2. Carrier Image

Image carriers' are the materials which carry an image for transfer directly or indirectly to the substrate. The most common type of image carrier is a plate and these are found in lithography, flexography, die stamping and pad printing.

However, image processing is more accurately defined as a means of translation between the human visual system and digital imaging devices. Image processing must be approached in a
manner consistent with the scientific method so that others may reproduce, and validate, one's results.

II. LITERATURE SURVEY

Ms. Ankita P. Baheti, Prof. Lokesh Singh, Prof. Asif Ullah Khan[1] - A Comparative Literature Survey on Various Image Encryption Standards - As multimedia applications are used increasingly, security becomes an important issue of communication and storage of images. Encryption is one of the ways to ensure high security. Images are used in many fields such as medical science, military; they are stored or transfer through network, security of such image data is important. Text encryption algorithms which have been already developed are not suitable for the image encryption, because image containing large amount of data means it contains number of pixels.

Mohammad Ali Bani Younes and Aman Jantan [2], Image Encryption Using Block-Based Transformation Algorithm, Encryption is used to securely transmit data in open networks. Each type of data has its own features, therefore different techniques should be used to protect confidential image data from unauthorized access. Most of the available encryption algorithms are mainly used for textual data and may not be suitable for multimedia data such as images.
Chandra Prakash Singar, Jyoti Bharti, R.K. Pateriya [3], A Substitute Method for Color Image Enciphering based on Cell Shuffling and Scan Pattern, In today's world, we use multimedia technologies in various daily applications to send vital information from one end to another side. However, security is a prime concern when data is sent over a public channel. There are various multimedia techniques to transfer data using sound, video, and images. However, these methods are not effective in security and performance.

Arian Dhini and Dhea Indriyanti [4], Clustering High-Dimensional Stock Data using Data Mining Approach, Clustering is helpful to pick out the acceptable stock for investors. Sadly, stock costs keep varied from time to time. Paper presents High Dimensional data cluster (HDDC), a model based mostly agglomeration supported Gaussian Mixture Model, with the Expectation-Maximization (EM) algorithmic rule.

Irfan Kamil, Bambang Pharmasetiawan [5], Fingerprint Presence Fraud Detection Using Tight Clustering on Employee's Presence and Activity Data, analyzing using a supervised algorithm cannot handle unlabeled data that generated uniquely for this case. Tight clustering method to detect fraud in fingerprint data using DBSCAN (Density-based spatial clustering of applications with noise) algorithm, as tight distance calculation removes non-fraud data because non-fraud data is generated to be unique naturally.

Qibing Zhu[6], Improvement of Spatial Data Clustering Algorithm in City Location, has become additional and additional mature, wide utilized in numerous fields. spatial bunch analysis formula will /deeply discovers the information that hidden within the geospatial data, determine the representative node of 1 or variety of spatial information assortment, discovery the law of the spatial distribution.

Bens Pardamean, Join W. C. Sigalingging, Kartika Purwandari, uhammad Fhadli, Shinta Nur Arizky[7], Data Mining for Predicting Customer Satisfaction Using Clustering Techniques, This study aims to work out the applying of the K-means, Spectral cluster (SC), and agglomerated cluster (AC) technique for activity client satisfaction. The cluster analysis supported agglomerated cluster approach performs moreover because the K-means approach to cluster an equivalent characteristics of the customer.

Saryu Chugh and Vanshita R Baweja[8], Data Mining Application in Segmenting Customers with Clustering, This paper describes concerning competition level that's raised between the organizations to retain the customers. Two-

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910022 |

phase cluster technique is applied for customers' retention. initial stage is employed to alter the k-means algorithmic program by utilizing a heuristic approach. collective cluster is employed to notice outliers.
Kais Allab, Lazhar Labiod, and Mohamed Nadif[9], A Semi-NMF-PCA Unified Framework for Data Clustering, his paper propose a completely unique to contemplate the cluster and therefore the reduction of the dimension at the same time. Indeed, our approach takes advantage of the mutual reinforcement between knowledge reduction and cluster tasks. the utilization of a low- dimensional representation is of facilitate in providing less complicated and additional explicable solutions.

Gang Li, Wenqian Jiang, Xiqiao Lin and Zhou Yang[13], An Electricity Data Cluster Analysis Method based on SAGA-FCM Algorithm, The key technology to analyzing electricity knowledge is cluster strategies, of that the standard method has already lost its agility and quality due to the increasing knowledge volume. This paper planned SAGA-FCM algorithm to enhance the information process results, which is a combination of Simulated hardening, Generic algorithmic rule and FCM (Fuzzy C Mean) algorithmic rule.

Rafal A. Angryk and Ruizhe Ma[14], Distance and Density Clustering for Time Series Data, we propose a Distance Density cluster methodology that's a medoid-based cluster with statistic knowledge density thought that provides cluster results in a hierarchy fashion. the space Density cluster technique on the UCR dataset demonstrates that cluster initialization is crucial in obtaining stable and higher results than random initialization on the average, and is additionally additional correct than traditional distance cluster.

C.K. Jha and Seema Maitrey[15], Handling Structured Data Using Data Mining Clustering Technique, Various application areas needed this method, thus, resulted into associate evolution of the many data processing ways. Though many data processing ways get evolved not all of them were capable to manage high voluminous knowledge. This paper place concentrate on CURE cluster technique that found appropriate for operating with massive databases.

III. COMPARATIVE ANALYSIS

Title	Techniques & Mechanisms	Parameter Analysis	Future Work
A Comparative Literature Survey on Various Image Encryption Standards.	As multimedia applications are used increasingly, security becomes an important issue of communication and storage of images.	Similar clustering structures, Better clustering performance	Network clustering accuracy can be further boosted
RNN-DBSCAN:A Density-Based Clustering Algorithm Using Reverse Nearest Neighbor Density Estimates	. Reverse nearest neighbor based clustering approaches (RECORD, IS-DBSCAN, and ISB-DBSCAN) along with DBSCAN and OPTICS	Problem complexity, improved ability, heterogeneous density, choice of k nearest neighbors.	RNN-DBSCAN is presented leveraging an existing approximate k nearest neighbor technique

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910022 |

A Similarity based K- Means Clustering Technique for Categorical Data in Data Mining Application	Similarity-based K-means Clustering (SKC)	Memory utilization, time consumption, overhead, computation complexity.	The results state that the developed study achieved98.45% accuracy for the publicly available dataset when comparing with the existing Techniques.
Clustering High-Dimensional Stock Data using Data Mining Approach	This paper Presents High Dimensional Data Clustering (HDDC), a model based clustering based on Gaussian Mixture Model, using the Expectation- Maximization (EM) algorithm.	.Dimension reduction, better quality, improve the performance	EM algorithm enables to handle the high- dimensional data better.

Fingerprint Presence Fraud Detection Using Tight Clustering on Employee's Presence and Activity Data	we propose a tight clustering method to detect fraud in fingerprint data using DBSCAN	Detect fraud, distance calculation	Distance calculation removes non-fraud data because non-fraud data is generated to be unique naturally.
Improvement of Spatial Data Clustering Algorithm in City	Spatial clustering analysis algorithm can deeply discover	Construct the spatial knowledge base, optimize the	This paper is based on the spatial data mining method, analysis and optimizes the spatial
Data Mining for Predicting Customer Satisfaction Using Clustering Techniques.	This study aims to determine the application of the K-means Spectral Clustering and Agglomerative Clustering method for measuring customer satisfaction.	customer satisfaction, cluster analysis	Result of customer satisfaction and provides improvement suggestion to the restaurant concerned.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910022 |

A Semi-NMF-PCA Unified Framework for Data Clustering	NMF, PNMF and Semi-NMF	Data reduction and clustering tasks	Good performances in terms of reparability between clusters, hence they can also be beneficial for visualization.
Dataset Designing of Software Architectures Styles for Analysis through Data Mining Clustering Algorithms	Software architecture is an important part of the software systems which states that how multiple components of the system interact with each other.	Software reusability, testing and maintenance	Researchers and software industrialists to define their own data set of their organizations for analysing the projects through data mining approaches.

IV. CONCLUSION

The proposed system provides an efficient cryptosystem using Block Transformation process and Random number generation to provide confidentiality service for data transmitted over a public network. Since the algorithm follows a new method of generating random numbers, it provides a better encryption compared to random number generation by blumblum algorithm. Also this method of implementing cryptosystem is more suitable for short and highly confidential messages. The proposed scheme is best with respect to the correlation between the original image and the encrypted image and also between the adjacent pixels of the encrypted image. The histogram of encrypted image is different from the histogram of the original image.

REFERENCES

1. S.Pavithra, Mrs. E. Ramadevi STUDY AND PERFORMANCE ANALYSIS OF CRYPTOGRAPHY ALGORITHMS International Journal of Advanced Research in Computer Engineering & Technology Volume 1,
2. Issue 5, July 2012 14 pp.82-86
3. Shanta, yoti Vashishtha on Evaluating the performance of Symmetric Key Algorithms:AES(Advanced Encryption Standard) and DES(Data Encryption Standard) in IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ,pp.43- 49
4. Monika Agrawal,Pradeep Mishra A Comparative Survey on Symmetric Key Encryption TechniquesInternational Journal on Computer Science and Engineering (IJCSE) Vol.4 No. 05 May 2012, pp.877-882.
5. Jawahar Thakur , Nagesh Kumar DES , AES and Blowfish : Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis in International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 1,Issue 2,December 2011),pp.6-12
6. Himani Agrawal and Monisha Sharma Implementation and analysis various symmetric cryptosystems in indian Journal of Science and Technology in Vol. 3 No.12 (Dec 2010) ISSN: 0974- 6846.pp.1173-1176
7. Aamer Nadeem and Dr M. Younus Javed , A Performance Comparison of Data Encryption Algorithms, IEEE, 2005.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542

|| Volume 9, Issue 10, October 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0910022 |

8. Ahmed Bashir Abugharsa, Abd Samad Bin HasanBasari and Hamida Almangush A New Image Encryption Approach using Block-Based on Shifted Algorithm, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.12, December 2011.
9. Aditee Gautam, Meenakshi Panwar and Dr.P.R Gupta A New Image Encryption Approach UsingBlock Based Transformation Algorithm , (IJAEST) international journal of advanced engineering sciences and technologies Vol No. 8, Issue No. 1, 090 096, 2011.
10. Sesha Pallavi Indrakanti and P.S.Avadhani Permutation based Image Encryption Technique, International Journal of Computer Applications (0975 8887) Volume 28 No.8, August 2011.
11. B.V.Rama Devi, D.Lalitha Bhaskari, P.Prapoorna Roja, P.S.Avadhani A New Encryption Method for Secure Transmission of Images, (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 09, 2010, 2801-2804.
12. Panduranga H.T and Naveen Kumar S.K, Hybrid approach for Image Encryption Using SCAN Patterns and Carrier Images , (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 02, 2010, 297-300.
13. Lala Krikor, Sami Babaet., Thawar Arif, and Zyad Shaaban Image Encryption Using DCT and Stream Cipher, European Journal of Scientific Research Vol.32 No.1 (2009), pp.47-57 ISSN 1450-216X
14. Bibhudendra Acharya, Saroj Kumar Panigrahy, Sarat Kumar Patra, and Ganapati Panda Image Encryption Using Advanced Hill Cipher Algorithm, International Journal of Recent Trends in Engineering, Vol. 1, No. 1, May 2009. [14]Mahmood Al-khassaweneh, Selin Aviyente,Image Encryption Scheme Based on Using Least Square Approximation Techniques IEEE Transactions, pp.108-111, 2008.
15. Mohammad Ali Bani Younes and Aman Jantan, An Encryption Approach Using a Combination of Permutation Technique Followed by Encryption IJCSNS, vol 3 no 4, April 2008.
16. Mohammad Ali Bani Younes and Aman Jantan, Image Encryption Using Block Based Transformation Algorithm IAENG, 35:1, IJCS_35_1_03, February 2008.
17. M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki A Modified AES Based Algorithm for Image Encryption, World Academy of Science, Engineering and Technology 27 2007.
18. Ameritech Mobile Communications et al., Cellular Digitalfacket Data Sjfstem Specifications: Part 406: Airlink Security, CDPD Industry Input Coordinator, Costa Mesa, Calif., July 1993.
19. Accredited Standards Committee X9, Working Draft: American National Standard X9.30- 1 993: Public Key Cryptography Using lrreversible Algorithms for the Financial Services Industry: Part 4: Management of Symmetric Algorithm Keys Using Diffie-Hellman, Am. Bankers Assoc., June 4, 1993.
20. FlPS Publication 180: SecureHashStandard(SHS), NIST, May 11, 1993.
21. E. Bihamand A. Shamir, "Differential Cryptanalysisof theFulll6- Round DES," Proc. Crypto 92, Advancesin Cryptology, Springer- Verlag, New York, 1993, to appear.
22. R.L. Rivest, The RC4 Encryption Algorithm, RSA Data Security, Inc., Mar. 12, 1992. NIST, "The Digital Signature Standard, Proposal and Discussion," Comm. ACM, Vol. 35,
23. No. 7, July 1992, pp. 36-54.
24. PKCS #3: Diffie-Hellman Key Agreement Standard, Version I .3, RSA Data Security, Inc., June 1991.
25. FlPSPublication46-1
26. :DataEncryptionStandardN. IST, Washington, D.C., Jan. 22, 1988; originally issued by the National Bureau of Standards.
27. Australian Standard 2805.5 1985: Electronics Funds Transfer- Requirements for Interfaces: Part 5-Data Encryption Algorithm, Standards Assoc. of Australia, North Sydney, NSW, 1985.
28. Accredited Standards CommitteeX3,ANSlX3.92: Data Encryption Algorithm (DEA), ANSI, New York, 1981.
29. W. Diffie and M.E. Hellman, "New Directions in Cryptography," /E Trans. information Theory, Vol. IT-22, 1976, pp. 644-654.
30. Hiral Rathod, Mahendra Singh Sisodia, Sanjay Kumar Sharma, Design and Implementation of Image Encryption Algorithm by using Block Based Symmetric Transformation Algorithm, International Journal of Computer Technology and Electronics Engineering (IJCTEE) Volume 1, Issue 3.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details