Research Article

A Systematic Review on Image Encryption Techniques

Gopal Ghosh[a], Kavita[b,*], Divya[a], Sahil Verma[b], M N Talib[c], Mudassar Hussain Shah[d]

[a] Lovely Professional University, Phagwara, 144411, India
[b] Department of Computer Science and Engineering, Chandigarh University, Mohali, Punjab, 140413, India
[c] Papua New Guinea University of Technology, Lae, PNG
[d] Department of Communication and Media Studies, University Of Sargodha, Sargodha

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 28 April 2021

Abstract:
In the form of text, audio, videos and photographs, the Internet is a commonly used tool to exchange details. The long-distance exchange of information on a wide network needs encryption to secure the information from unauthorized access. The reliability of the network plays an important role in protecting data on an insecure network. Many encryption solutions have been discovered to protect the data on the network, and recent creative encryption schemes have been in demand since e-commerce e-banking and multimedia technologies are viewed on a regular basis on the internet. Cryptographic coding methods have lately been used primarily to protect unauthorized access to knowledge on an insecure network. The researchers also established many cryptographic strategies for protecting and efficiently transmitting knowledge on an insecure network. Image encryption techniques are commonly used by all cryptographic techniques to transmit photos on an insecure network. The purpose of this paper is to demonstrate the few encryption techniques that are used on an insecure network to encrypt the image. To encrypt the image, this paper proposes a new encryption technique. The suggested approach encrypts the image using Wavelet Transform, the Chaotic Mechanism, along with the production of the image fingerprint using the Hash function to be sent to the recipient. The suggested procedure, along with anonymity, often protects the image's encryption.

Keywords: Image Encryption; Chaotic System; Wavelet Transform; Hash Function; Fingerprints;

1. Introduction:

Over the past decade, the use of smartphones, the Internet and multimedia technology has demonstrated widespread interest. The need for users is not only restricted to text, but also to share knowledge about the broad network, i.e., Music, video and video are often used on the phone. Therefore, utilizing images and video [10], the need for a safe network has become a necessity. Photographs are actually being sent and treated electronically such that the information in the image are subject to modification or alteration by unauthorized access [9]. Increased images security is needed to incorporate and progress network infrastructure. Digital imaging encryption was one of the strong protections for image security and was the topic of research. The Image Encryption techniques are classification in shown in Fig: 1

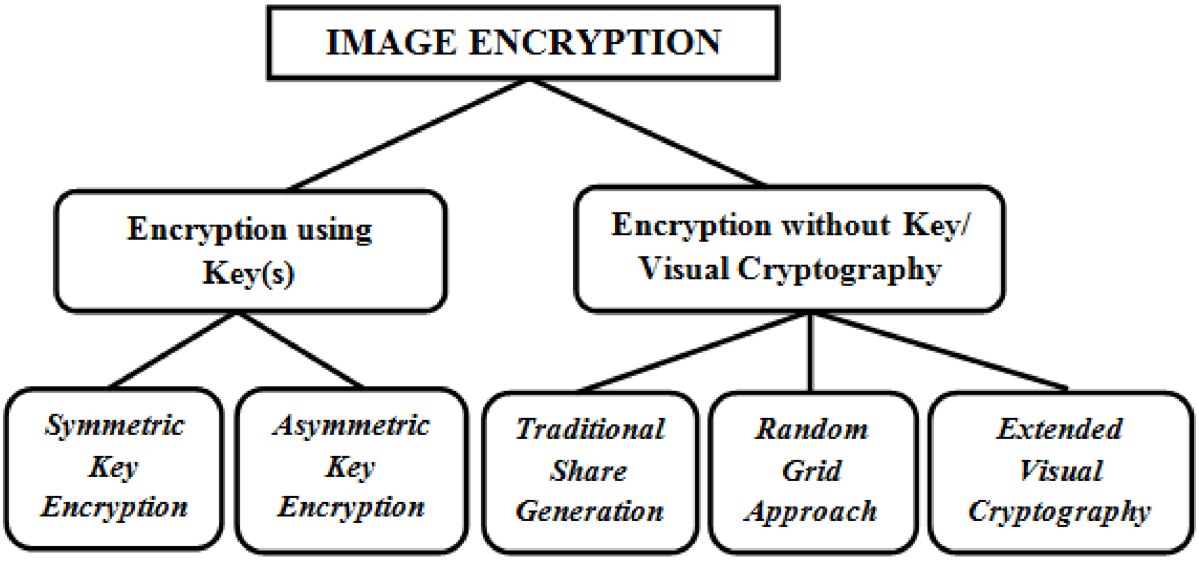


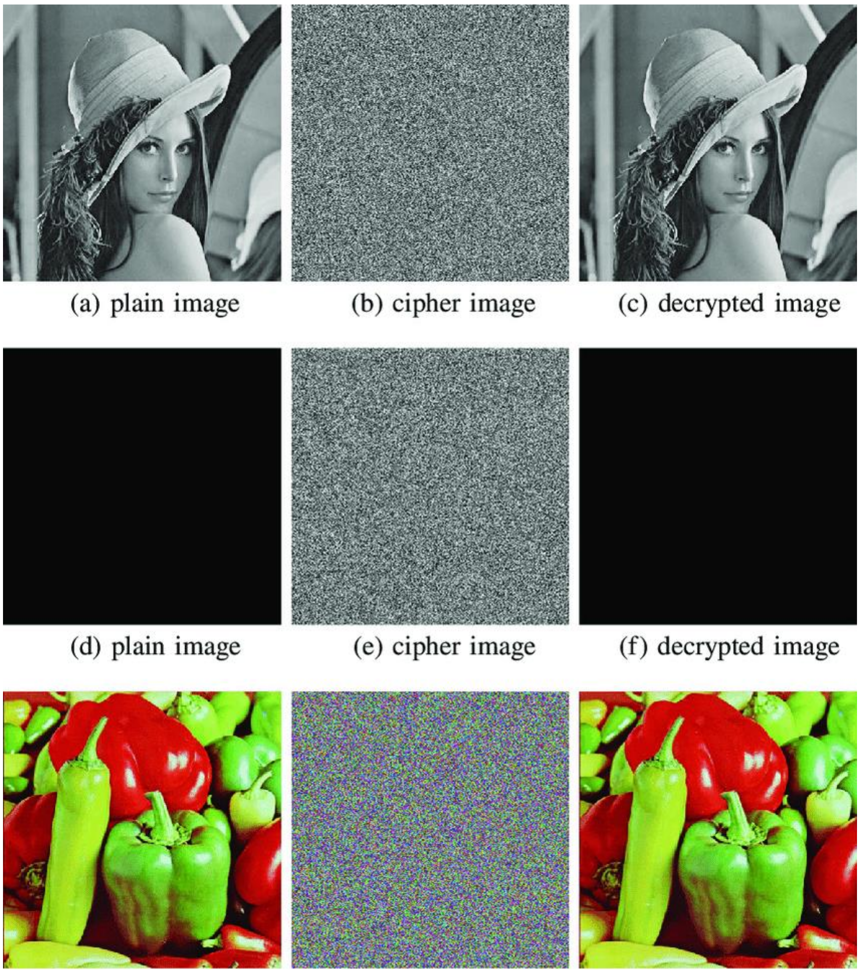
IMAGE ENCRYPTION
Encryption using Key(s)
Encryption without Key/ Visual Cryptography
Symmetric Key Encryption
Asymmetric Key Encryption
Traditional Share Generation
Random Grid Approach
Extended Visual Cryptography

Fig: 1 Image Encryption techniques

In recent years, the requirement for the sharing or transmission of image data on the internet has contributed to a great deal of interest in image encryption. A number of researchers have also introduced methods for image encryption [6]. Modem cryptography is one method that guarantees privacy, integrity and authenticity. Cryptography provides some programming complicated algorithms like DES, Concept and RCS, but they are called complex. but they are called complex. However, algorithms of unorderly encryption also have machine procedures considered reliable and most popular over these years, instead of implementing stream or block cryptosystems [9].

Everywhere the existence of disorder is found, the idea of the dynamic structure is considered to be the most complicated. Dynamic system research aims at calculating the actual or incremental appearance of the iterative operation. Chaos is a random sport which means that there is no intervention in linearity, which creates random phenomenon in a certain nonlinearity environment without other random variables. The disorderly system's creation is highly sensitive to its initial conditions; the future action of the messy system is therefore hard to predict [6].

For multi-frequency channels, Wavelet transform is a decomposition process [10]. It specifies the empirical form of time frequency and multi-resolution and is used to classify partial time and frequency domain characteristics. The keynote of the transformation in the Wavelet is the idea of decomposing the painting into a sub-image which offers information of the frequency and then processes the factor. Cryptography hash functions are a popular tool. The hash values created by the message represent longer messages themselves. The Fingerprint features are used as high-performance Hash functions that are a gateway to accessing the details showing the immutability and individuality of those that supply patient information with secrecy and reliability [l] and play an important role in checking the authenticity of the message and its digital signatures [8]. The Image Encryption flow is shown in Fig: 2.


(a) plain image (b) cipher image (c) decrypted image

(d) plain image (e) cipher image (f) decrypted image

Fig: 2 Image Encryption flow

2. Literature Review:

A new medical imaging safety and security policy was introduced for Viswanathan P, Venkata Krishna.p [l]. The author used the traditional FED watermarking system for security purposes. The Fingerprint, Coding and Dual Watermarking System method is used for securing Teleradiology. The fingerprint algorithm you propose would be used to retrieve the fingerprint picture along with the watermarking of the image encryption. The fingerprinting algorithm offers a new technique for testing and verifying the identity of the patient.

In [2] have a modern way of communicating and transmitting an image across the network. The proposed approach also implemented a framework. A secure network sharing fingerprint picture. The reversible hidden transformation is applied to the fingerprint picture, along with partly linear chaotic map. The secure picture is distributed on the compromised network. The original fingerprint image is reconstructed by the reverse process on the recipient hand.

In [3] introduced a modern solution to a chaotic map with shifting parameters. The suggested approach has two essential features: simultaneous encoding and message extension. The method uses a disorderly asymmetric tent map and piece-wise linear map to convert extended messages blocks iteratively into an ASCII code in which parameters are dynamically modified with the position of the respective message block index and the decimal portion is then generated which is then cascaded to the integer. The theoretical examination and simulation of the system's machine disclose a rather effective process.

Chaotic frames and wavelet transition are part of the proposed platform. The suggested solution creates unequal sequences by introducing the logistic map. This refers to the plaintext being provided. The distributed plaintext is then followed by the transition of the wavelet and the disruptive disorder. The Inverse Wavelet Transform IS was then used to reconstruct the encrypted image. The algorithm testing is carried out on the basis of the key study, which ensures that a small alteration of the key may benefit from major changes, a gray-level histogram, anti-noise test and anti-cutting tests. The analysis showed that pre-encryption diffusion decreased the strength of the ambiguity encryption attack. Due to unsafe cryptography, the result of diffusion is secret and the unfeasible features of the file may be deciphered.

A new digital watermarking technology was developed by Lina [5]. The author used in the essay to establish interactive watermarks the concept of distinct wavelet transformation and chaos. First the discrete wavelet transformation is applied to the image, then the low-frequency part is removed, and the mess sequence is applied to encrypt the small-frequency element. The first image is used for extraction, and this is a method of non-blind recognition. The NC coefficient and high noise to signal ratio test the device (PNSR). The results suggested that the mixture of a combined technical photographic culture, a noise attack, a filtration, etc. The influence of the watermark image has been quite high [6]. For the data encryption method, the author used the logistic solution of chaos. The analysis of the algorithm takes place on the following principles, such as randomness, resemblance and complexity. The chaos sequence simulation has shown that it satisfies the criteria of the encryption algorithm.

In [7] introduced a method for the encryption of images. The method suggested uses discreet chaotic diagrams, which combine permutation and substitute techniques. A standard Lena picture verified the algorithm that indicated that the original image was transformed by chaotic series into random image. The operation was effective and reasonably healthy.

In [8] has given a creative approach for uniform hash function decoding into propositional logic formulas. The technique is applied to the C vocabulary. The writers have built a modern approach to deliver rough and satisfying propositional formulas and difficult and incomplete propositional formulas. By using these formulas, the contrast of different functions can be done and disadvantages can be identified.

The encryption of images linked to the Baker chart has been enhanced by [9]. Unfortunately, methods for the encryption of photos have been created and tested to suggest that certain keys have generated poor encryption. The algorithm has therefore been improved by adding new features, such as changing the meaning of grayscale pixels, transposing the pixels by moving and binding a password to the image to maximize the encryption power. The method is tracked by drawing the pixels and results grayscale meaning.

The literature review indicates that several methods have been established to encrypt the image for network transmission. The principle of chaos and wavelet transformation was found for the encryption of pictures. The literature survey reveals that the privacy of the image was preserved, but the integrity of the image was not upheld. A modern method to protecting integrity and privacy has been introduced in this article. The approach proposed uses photo fingerprints to shield the identification of the picture inside a protected network. Image encryption techniques is useful in several methods for various applications [21-23] such as in medical imaging as well. A range of its usefulness is available in many cases in the literature.

Recent studies in Image Encryption Techniques

Recent studies in Image Encryption Techniques are tabulated in Table: 1

Table: 1 Recent studies in Image Encryption Techniques

S.No	Authors	Year	Remarks
1	T. S. Ali; R. Ali [11]	2020	Author Proposed "A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map"
2	P. Li; K. -T. Lo [12]	2020	Author presented "Survey on JPEG compatible joint image compression and encryption algorithms"
3	N. A. Loan; N. N. Hurrah; S. A. Parah; J. W. Lee; J. A. Sheikh; G. M. Bhat [13]	2018	Author Proposed "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption"
4	E. A. Umoh; O. N. Iloanusi; U. A. Nnolim [14]	2020	Author presented "Image multi-encryption architecture based on hybrid keystream sequence interspersed with Haar discrete wavelet transform"
5	H. Diab [15]	2018	Author presented "An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations"

6	T. Shah; T. U. Haq; G. Farooq [16]	2020	Author Proposed “Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation”
7	W. Feng; Y. He [17]	2018	Author Proposed “Cryptanalysis and Improvement of the Hyper-Chaotic Image Encryption Scheme Based on DNA Encoding and Scrambling”
8	M. Kaur; V. Kumar [18]	2018	Author studied “Colour image encryption technique using differential evolution in non-subsampled contourlet transform domain”
9	J. He; S. Huang; S. Tang; J. Huang [19]	2018	Author Proposed “JPEG Image Encryption With Improved Format Compatibility and File Size Preservation”
10	X. Zhang; X. Wang [20]	2018	Author Proposed “Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem”

3. Conclusion:

This paper presents the literature review on image encryption techniques. Using chaotic sequence and wavelet transform, the image encryption techniques were applied. The analysis of the paper indicates that the techniques for protecting the security of the image. This paper demonstrated the encryption techniques that are used on an insecure network to encrypt the image. To encrypt the image, this paper proposes a new encryption technique. The suggested approach encrypts the image using Wavelet Transform, the Chaotic Mechanism, along with the production of the image fingerprint using the Hash function to be sent to the recipient. Finally, recent studies in Image Encryption Techniques are tabulated.

References:

[1] P. Viswanathan, Member, P. Venkata Krishna, "A Joint FED Watermarking System using Spatial Fusion for Verifying the Security issues of Teleradiology", IEEE JOURNAL OF BIOMEDICAL AND HEALTH INFORMATICS, pp. 1-12,2013.

[2] Gaurav Bhatnagar and Q. M. Jonathan Wu, "Chaos-Based Security Solution for Fingerprint Data During Communication and Transmission", IEEE TRANSACTIONS ON INSTRUMENT A TION AND MEASUREMENT, VOL. 61, NO.4, pp. 876-887 APRIL 2012.

[3] Yantao Li, Di Xiao, Shaojiang Deng, Qi Han and Gang Zhou, "Parallel Hash function construction based on chaotic maps with changeable parameters", SPRINGER, Neural Computing and Applications, pp. 1305-1312, 17 February 2011.

[4] Runhe Qiu, Y uzhe Fu, Y un Cao, "Image Encryption Research based on chaotic sequences and wavelet stransform", IEEE, pp.1511-1516, 2010.

[5] Qiang Wang, Qun Ding, Zhong Zhang, Lina Ding, "Digital Image Encryption Research Based on DWT and Chaos", IEEE Computer Society Fourth International Conference on Natural Computation, pp. 494-498, 2008.

[6] Gannan Yuan, Research on Data Encryption Technology Based on Chaos Theory", IEEE Computer Society Eighth ACIS International Conference on Sofuvare Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, pp. 93-98, 2007.

[7] Guosheng Gu and Guoqiang Han, An Enhanced Chaos Based Image Encryption Algorithm", IEEE Computer Society First International Conference on Innovative Computing, Information and Control, 2006.

[8] Gopal Ghosh et al 2020 IOP Conf. Ser.: Mater. Sci. Eng. 993 012062.

[9] Mazleena Salleh Suhariah Ihrahim Ismail Fauzi lsnin, Enhanced Chaotic Image Encryption Algorithm Based on Baker's Map", IEEE, pp. 508-511, 2003.

[10] A. Diro, H. Reda, N. Chilamkurti, A. Mahmood, N. Zaman and Y. Nam, "Lightweight Authenticated-Encryption Scheme for Internet of Things Based on Publish-Subscribe Communication," in IEEE Access, vol. 8, pp. 60539-60551, 2020, doi: 10.1109/ACCESS.2020.2983117.

[11] T. S. Ali and R. Ali, "A Novel Medical Image Signcryption Scheme Using TLTS and Henon Chaotic Map," in IEEE Access, vol. 8, pp. 71974-71992, 2020.

[12] P. Li and K. -T. Lo, "Survey on JPEG compatible joint image compression and encryption algorithms," in IET Signal Processing, vol. 14, no. 8, pp. 475-488, 10 2020.

[13] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh and G. M. Bhat, "Secure and Robust Digital Image Watermarking Using Coefficient Differencing and Chaotic Encryption," in IEEE Access, vol. 6, pp. 19876-19897, 2018.

[14] A. Umoh, O. N. Iloanusi and U. A. Nnolim, "Image multi-encryption architecture based on hybrid keystream sequence interspersed with Haar discrete wavelet transform," in IET Image Processing, vol. 14, no. 10, pp. 2081-2091, 21 8 2020.

[15] H. Diab, "An Efficient Chaotic Image Cryptosystem Based on Simultaneous Permutation and Diffusion Operations," in IEEE Access, vol. 6, pp. 42227-42244, 2018.

[16] T. Shah, T. U. Haq and G. Farooq, "Improved SERPENT Algorithm: Design to RGB Image Encryption Implementation," in IEEE Access, vol. 8, pp. 52609-52621, 2020.

[17] W. Feng and Y. He, "Cryptanalysis and Improvement of the Hyper-Chaotic Image Encryption Scheme Based on DNA Encoding and Scrambling," in IEEE Photonics Journal, vol. 10, no. 6, pp. 1-15, Dec. 2018, Art no. 7909215.

[18] M. Kaur and V. Kumar, "Colour image encryption technique using differential evolution in non-subsampled contourlet transform domain," in IET Image Processing, vol. 12, no. 7, pp. 1273-1283, 7 2018.

[19] He, S. Huang, S. Tang and J. Huang, "JPEG Image Encryption With Improved Format Compatibility and File Size Preservation," in IEEE Transactions on Multimedia, vol. 20, no. 10, pp. 2645-2658, Oct. 2018.

[20] X. Zhang and X. Wang, "Digital Image Encryption Algorithm Based on Elliptic Curve Public Cryptosystem," in IEEE Access, vol. 6, pp. 70025-70034, 2018.

[21] Kumar, T., Pandey, B., Mussavi, S. H. A., & Zaman, N. (2015). CTHS based energy efficient thermal aware image ALU design on FPGA. Wireless Personal Communications, 85(3), 671-696.

[22] S. Saeed and A. B. Abdullah, "Investigation of a Brain Cancer with Interfacing of 3-Dimensional Image Processing," 2019 International Conference on Information Science and Communication Technology (ICISCT), 2019, pp. 1-6, doi: 10.1109/CISCT.2019.8777404.

[23] Ahmad, M., Zaman, N., Jung, L. T., Ilyas, M., & Rohaya, D. A. (2014). An Integrated Approach for Medical Image Enhancement using Wavelet Transforms and Image Filtering. Life Science Journal, 11(6), 445-449.