IJMTST is UGC Approved Journal with Journal Id: 43137

International Journal for Modern Trends in Science and Technology, 8(S03):173-177, 2022
Copyright © 2022 International Journal for Modern Trends in Science and Technology
ISSN: 2455-3778 online
DOI: https://doi.org/10.46501/IJMTST08S0339
Available online at: https://www.ijmtst.com/vol8si03.html

SIE: A Novel Cryptosystem to Secure Confidential Images

M. Harini Naga Sai*, Dr. Sri Ram Chandra Polisetty*, Dr. G. Venkateswara Rao#, Dr. G.V.Swamy#

*Department of Computer Science and Engineering, Godavari Institute of Engineering and Technology (A), JNTUK, Kakinada.
Faculty of Engineering, GITAM-Deemed to be University, Visakhapatnam, A.P., INDIA.

To Cite this Article
M. Harini Naga Sai, Dr. Sri Ram Chandra Polisetty, Dr. G. Venkateswara Rao and Dr. G.V.Swamy. SIE: A Novel Cryptosystem to Secure Confidential Images. International Journal for Modern Trends in Science and Technology 2022, 8(S03), pp. 173-177.https://doi.org/10.46501/IJMTST08S0339

Article Info
Received: 26 April 2022; Accepted: 24 May 2022; Published: 30 May 2022.

ABSTRACT

Image encryption may be defined as the process of encoding confidential image(s) with the help of an encryption algorithm in such a way that it is inaccessible to unauthorized users. While transferring such images across the social networksor its applications, it is necessary to have a highly secured cryptosystem. Though several encryption techniques are publicly available, each of them has their own strong and fragile focuses. This paper depicts the newly proposed cryptosystem named as Secured Image Encryption with an acronym SIE. The input image undergoes series of operations to get converted into its encoded form. The model results regarding histogram and correlation analysis of encrypted as well original images illustrated in the further sections are evident that the proposed cryptosystem is large enough to protect the encrypted image.

1.INTRODUCTION

We are living in the digital information age where digital objects viz., photos, audio, documents are processed by digitization.[11In transferring such critical pictures across the network, may sometimes get into the hands of unauthorized personal which may lead to financial or political loss. Therefore, new security research is in order of the day. Image encryption is one of the most secure ways to protect your images.[12] The encryption of the transmitted data is converted to unknown content using some private key. Not only does it secures the image but also withstand against the cryptographic attacks.

2. Literature Survey

[1] Over the last few decades, data has become progressively important in many aspects of human life. Data has grown exponentially in recent years as a result of the implementation of new applications. Cloud computing is a technology that permits us to store massive volumes of data in the cloud. This research proposes a novel lightweight cryptographic technique that can be used to safeguard cloud computing applications and promote data security. The algorithm is a 16-byte (128-bit) block cipher that encrypts data with a 16-byte (128-bit) key. Shannon's theory of diffusion and confusion is integrated into this algorithm.

[2] This white paper focuses primarily on the various encryption algorithms used to encrypt and decrypt images in the field of image security. As information technology becomes more widespread, security has become a major concern. . Cryptography refers to the study of aspects related to information security mathematical techniques, such as data confidentiality, data integrity, and data authentication.

[3] In particular, this paper focuses on the exclusive form of image encryption and decryption strategies. In addition, As virtual strategies for transferring and storing photos increase, protecting the confidentiality, integrity,

and reliability of photos becomes an important issue. Various strategies can be observed from time to time to encrypt images to make them even more secure.

[4] Image encryption is one of the most commonly used methods for hiding information. Certainly, a novel in this article, The pixel in the image and the second pixel rotate the circle to the right of these bits. In both of these encryption phases, the process is repeated many times. Keyspace analysis, key sensitivity analysis, statistical analysis. Performance experiments have shown that the proposed method is appropriate.

[5]This new algorithm performs lossless imagesEncryption combined with key-dependent variable-length XOR Encryption with Sbox replacement. This algorithm isimplemented and tested by running various permutations Empirical analysis of XOR encryption and Sbox replacementView with different types of test images of different sizes this new algorithm is an effective and statistically robustattack. The idea presented by this algorithm isGeneralized and applied to non-input data.

[6]This document aims to improve the security level of data protection provided by grayscale digital image encryption. The converted image is divided into blocks of 2 pixels x 2 pixels, and each block is encrypted with an XOR 48-bit key. The total size of the algorithm keys is 32. Because of this strong correlation of each pixel, you can predict from the value of that neighbor.

[7] Lightweight cryptography has a primefunction in cybersecurity for clevertowns and the Internet of Things. In this article, we'veadvanced a lightweight cryptographic set of rules, and via studies, analysis, and assessment with differentlight-weight cryptography algorithms display that the proposed set of rules is efficient.

[8] As a future-oriented technology, the Internet of Things (IoT) must connect billions of objects. Secure IoT is a lightweight encryption technique proposed in this paper (SIT). This is a 64-bit block cipher that encrypts data with a 64-bit key. Feistel and a uniform forward transport network are combined in the algorithm architecture. The approach achieves crucial security in just five encryption rounds, according to simulation data.

[9] Authenticated encryption meets the fundamental needs of reliability and confidentiality in information infrastructure. This document provides Ascon128 and Ascon128a specifications.It also specifies the hash function AsconHash and the extensible output function AsconXof. In addition, it complements the specification by providing a detailed overview of existing cryptanalysis and implementation results.

3. Architecture of the Proposed System

The architecture ofthis image cryptosystem explains the deep flow of the encryption and the decryption processes. The main aim of this SIE cryptosystem is to convert the original image into its encrypted form at the sender end. In contrast, the encrypted image should be reverted back to the original image at the receiver end.

In this SIE cryptosystem, the original image is converted into Base 64 from followed by binary code. This binary code undergoes series of operations embodied in encryption algorithm to generate an encrypted image. The image decryption in SIE ignites by performing the quite reverse processes of encryption as described in Figure 1.

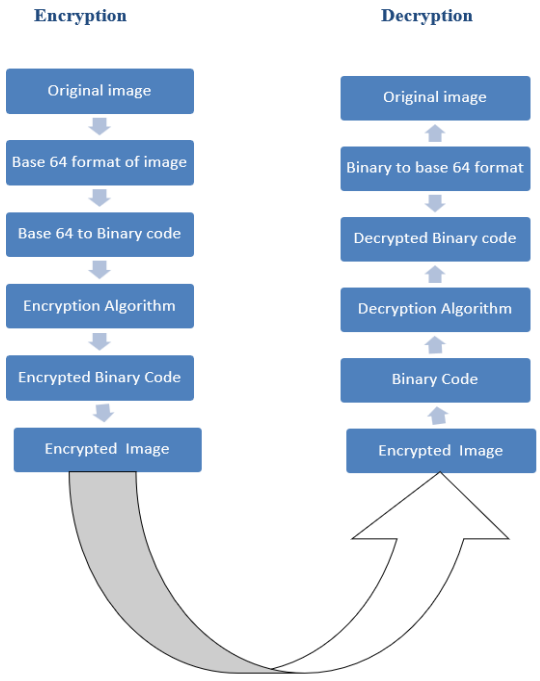


Figure 1: Architecture of the proposed system

3.1 Key Generation

The keys can be considered as most essential part of the encryption and decryption processes of any cryptosystem. The detailed key generation of SIE is depicted as follows.

- The 64-bit cipher key (k_c) is split into 4 segments of 16 bits each.
- The substitution function (F) is applied over all 4 segments as shown in Figure-2.

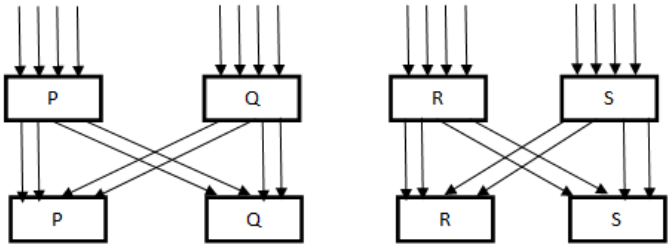


Figure 2: Substitution function

- The shift operation is performed to the result obtained by the substitute function (>>4 and >>6 simultaneously)
- The output of shift operation is converted as an array of 4 X 4 matrix.
- The Rotations are applied on the matrix to get the keys K1, K2, K3, K4.
- The combination of keys K1 X-OR K3 is K5, K2 X-OR K4 is K6, K5 >> 5 is K7, K6>>9 is K8. The generated keys are K1, K2, K3, K4, K5, K6, K7, K8.

3.2 Proposed Encryption and Decryption Algorithms:

Encryption is the process of striving or encoding data so as to prevent anyone other than the intended recipient of the data from reading the data that was communicated. The SIE encryption Algorithm is the contiguous process after keys (K1, K2, K3, K4, K5, K6, K7, K8) that are generated by the key generation algorithm. To encode the original image, SIE cryptosystem is encompassed with X-OR, left shift, swapping, and shifting operations, 8 rounds with 8 keys in-order to increase the confusion and diffusion.

Decryption may be considered as the inverse process of encryption with slight changes in it. The encoded image is taken as an input and transmogrified into base 64 followed by binary. The order of keys that are used in decryption is from K8 to K1 for round1 to round8 respectively. The obtained binary undergoes the conversion of base-64 followed by original image.

As a whole, the detailed Key Generation, encryption and decryption of SIE are depicted below in figures 3, 4 and 5 respectively.

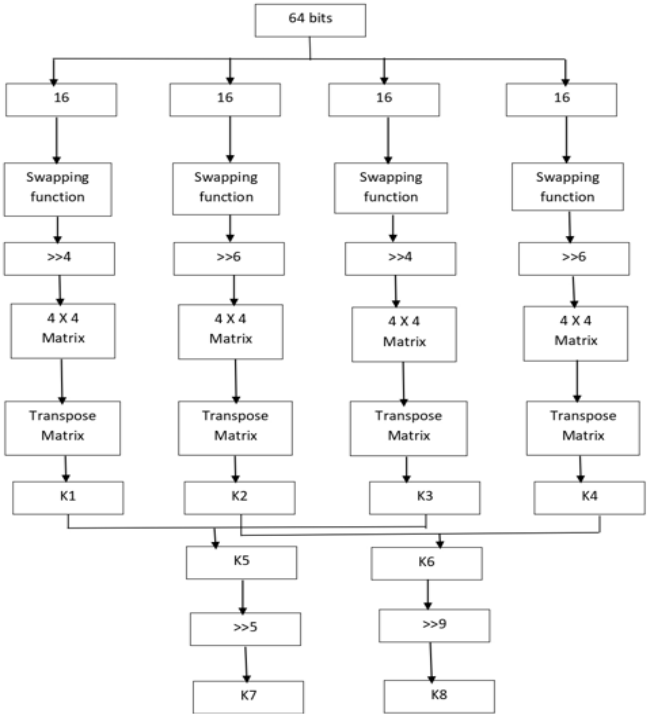


Figure 3: SIE - Key Generation

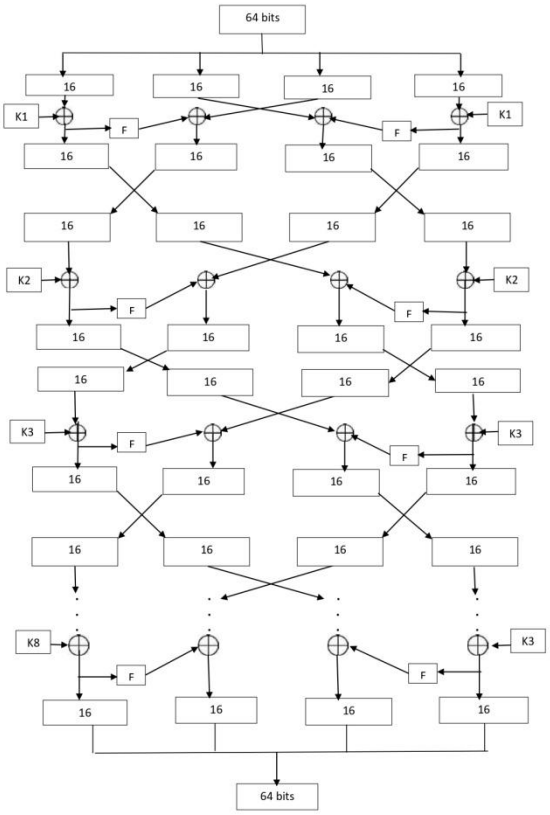


Figure 4: : SIE - Encryption

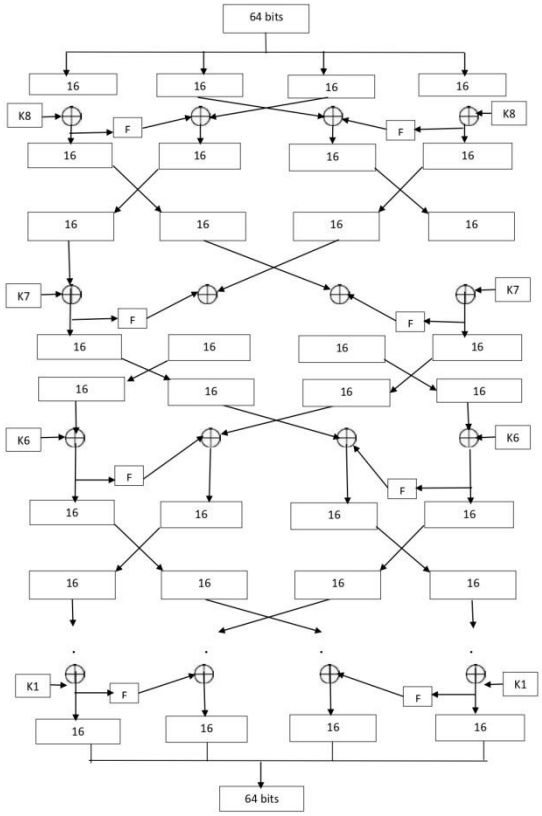


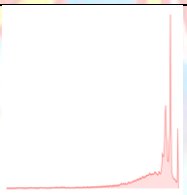
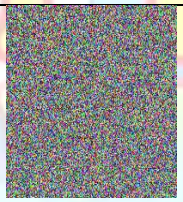
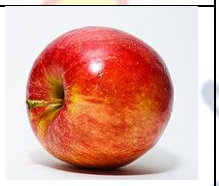
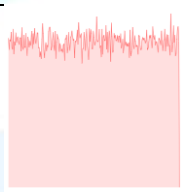
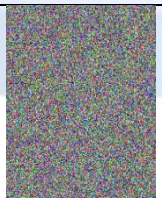
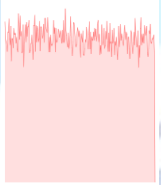
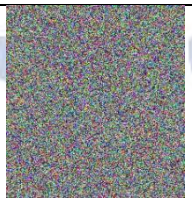
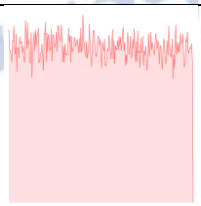
Figure 5: : SIE - Decryption

4. Results and Discussion

To show the efficiency of encrypted images, histogram analysis can be considered as one of the most straight forward strategies. Since a good picture encryption procedure will overall scramble a unique picture to sporadic like, seeing a reliably scattered histogram for an encoded image is needed. Histogram analysis of the plain and encoded images is embodied in section 4.1.

4.1 Histogram analysis of the plain and encoded images

Table 1 Histogram Analysis of the plain and encoded images

Image No.	A Plain Image	B Histogram of A	C Encoded Image of A	D Histogram of C	E Decoded Image of C
1					
2					
3					
4					

The histogram of the encrypted images 1 through 4 is uniform and significantly differs from that of the Plain one. Thusly, no indication of the plain picture is existent to be utilized by the measurable assaults.

The histogram is approximated by a uniform distribution. The uniformity is justified by chi-square test in equation.

$$X^2 = \sum_{k=1}^{256} \frac{(V_k - 256)^2}{256} \qquad \text{.....1}$$

Where count of gray scale areas is denoted by k and each area's repetition by V_k.

Table 2: Chi-Square values-Histogram approximation

Chi-square/ Image Number	1	2	3	4
Image before encryption	29,384	213843	145214	54125
Image encrypted using SIE Cryptosystem	225.5162	242.5486	229.7452	259.6541

The average Chi-square value for the encrypted images of the proposed cryptosystem SIE is 239.366. The result of this test demonstrated that the histogram of the encrypted image is uniform.

5. CONCLUSIONS

Safeguarding pictures in the present advanced world has become vital in light of quick expansion in the computerized correspondence. In this context authors made a step ahead towards the design of a new cryptosystem SIE, which aimed at encrypting an image so as to protect it from unauthorized users. The histogram analysis and Chi-Square test results embodied in results and discussion are evident that the proposed cryptosystem can withstand to certain intruder's attacks.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

[1] Fursan Thabit, Sharaf Alhomdy, Abdulrazzaq H.A. Al-Ahdal, Dr. Sudhir Jagtap, A new lightweight cryptographic algorithm for enhancing data security in cloud computing,

[2] rasenjit Kumar Das, Mr. Pradeep Kumar, and Manubolu Sreenivasulu, Image Cryptography: A Survey towards its Growth, 2014

[3] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya, A Survey on Different Image Encryption and Decryption Techniques, 2013.

[4] Mohammed Abbas Fadhil Al-Husainy, A Novel Encryption Method for Image Security,2011

[5] Abdelfatah A. Tamimi and Ayman M. Abdalla, An Image Encryption Algorithm with XOR and S-box, 2016.

[6] Rinki Pakshwar, Vijay Kumar Trivedi, Vineet Richhariya, Image Encryption Using Random Scrambling and XOR Operation. 2013.

[7] Ahmed Mohsin Abed, Ali Boyacı, A Lightweight Cryptography Algorithm for Secure Smart Cities and IOT, 2022

[8] Muhammad Usman, Irfan Ahmed†, M. Imran Aslam, Shujaat Khan∗and Usman Ali Shah, 2017

[9] Christoph Dobraunig, Maria Eichlseder, Florian Mendel · Martin Schläffer, Lightweight Authenticated Encryption, and Hashing.

[10] Parvathi, D. S. L., Leelavathi, N., Ravikumar, J. M. S. V., & Sujatha, B. (2020, July). Emotion Analysis Using Deep Learning. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 593-598). IEEE.

[11] Kumar, J. R., Sujatha, B., & Leelavathi, N. (2021, February). Automatic Vehicle Number Plate Recognition System Using Machine Learning. In IOP Conference Series: Materials Science and Engineering (Vol. 1074, No. 1, p. 012012). IOP Publishing.