Secure Image System

Koushik K[1], Sirajul Hassan T.K[2], Ms.Vijetha[3]
[1, 2] Dept of Computer Science and Engineering
[3]Associate Professor, Dept of Computer Science and Engineering
[1, 2, 3] Srinivas Institute of Technology, Valachil, Mangaluru-575007

Abstract- *Images plays important role in information sharing eg, whatsapp, facebook etc., all social medias. Images are the great source, but the problem we face is storing large size of images is difficult. Any communication media that contains images, suffer from two tough problems: large size and data in clear give raise to information leak. Therefore, photos should be reduced to smaller sizes and converted into form that gives no chance to data insecurity. Hence we propose a new photo compression and encryption scheme that relies on lossy JPEG standardization which tries to get a good balance between both of these operations. We generate a secrete key from the plain image itself via Blake2 hash algorithm, so our system is image-content-adaptive in nature. To overcome the problem of security of key we enable using hashing property. Various tests are carried out to make sure that our system is strongly persistence to several crypt-analysis techniques.*

Keywords- Data JPEG; Blake2; Compression, hashing value; secrete key;

I. INTRODUCTION

Digital images used in many communication applications, therefore the protection the content of these images become very important. Image encryption is a technique which coding the original image to another un-understanding image Image form a major part of the data that is being transmitted in various social media platforms. Hence encrypting of images becomes more important. In the proposed project BLAKE2 hash algorithm is used for generating the secret encryption key from plain text. Along with this three different encrypting techniques have been used namely alternating new orthogonal transforms transformation, DC coefficient encryption and AC coefficients encryption. To obtain the decrypted form of image same operations re applied in reverse order. Protecting the performance of the system against the different types of attack is a major task.

Protecting the performance of the system against the different types of attack is amajor task. This lacked in many compression-encryption techniques leading to failure of the system. However, the process of generating encryption key from raw image can increase the diffusion property of cryptosystem. By increasing the AC coeffcients category without making any change to the format of data of encrypted bit stream data hiding techniques can be generated. By implementing the proposed system we can achieve greater amount of encryption and compression.

II. BACKGROUND

Lingfeng Liu and Suoxia Miao [1], proposed a new image encryption algorithm based on parameter varied logistic chaotic map and dynamical algorithm. It can cure the weaknesses of logistic map and resist the phase space reconstruction attack. We use the parameter-varied logistic map to shuffle the plain image, and then use a dynamical algorithm to encrypt the image. The experiment results show that this algorithm is with high security and can be competitive for image encryption.

In [2], Kumar et al. introduced a unique technique to encrypt images in two stages using pixel transposition and Lehmer randomization concept. In the _rst stage, a standard sorting algorithm is applied on pixel of original image. Duplicate pixel values are eliminated to generate initial transposed image. Image pixel position values are used as unique security attribute and are fetched from the image with respect to initial transposed im- age and are written as textile. The second stage provides an extra level of security to position values (security attributes) and initial transposed image. The size of generated cipher image is several times smaller than that of original image. The analysis shows that the algorithm is resistant to statistical and differential attacks.

In this [3] paper, Hiba Abdel-Nabi and Ali Al-Haj introduced an efficient crypto-water marking algorithm to secure medical images transmitted in tele-medicine applications. The proposed algorithm uses standard encryption methods and reversible watermarking techniques to provide security to the transmitted medical images as well as to control access privileges at the receiver side. The algorithm jointly embeds two watermarks in two domains using encryption and reversible watermarking to avoid any interference between the watermarks. Cryptographic techniques scramble the medical image to achieve confidentiality, and use digital signatures to provide authenticity and integrity.

Mohammed M. Siddeq and Marcos A. Rodrigues [4], proposed a new strategy for image compression whose quality is shown through accurate 3D reconstruction from 2D images. The technique depends on the discrete cosine transform (DCT) together with a high-frequency minimization encoding algorithm at compression stage and a new concurrent binary search algorithm at decompression stage. Results show that the proposed compression technique is perceptually better than JPEG with proportional quality to JPEG2000.

Laiphrakpam Dolendro Singh et al. [5], proposed a new encryption scheme using multi image compression. Cipher images that are generated from the usage of encryption algorithms are noise-like image, which suggests a clear indication for the presence of encrypted facts. The noise-like images reasons an adversary to carry out attacks.

III. MODULAR DIAGRAM

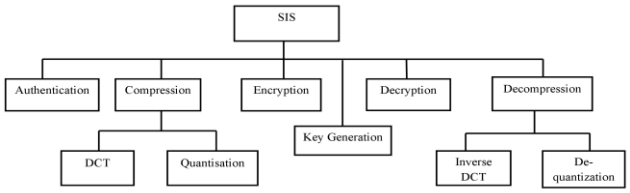

Figure 1: Modular Diagram of Secure Image System.

Modular diagram is a representation for independent modules that performs essential operations of the system. Figure 1 describes the modular diagram of our Secure Image System. SIS is organized into several independent modules which represents the essential operations of our system. This involves Authentication module for user login operation, Compression module represents the compression function and also it has sub-modules being identified as DCT and Quantization, Encryption and Decryption modules represents the basic functions of the system for enciphering and de-ciphering process, Key generation module generates keys required through the operation of the system and finally decompression block indicating the decompression operation with sub modules being identified as Inverse-DCT and De-quantization.

IV. ALGORITHM REVIEW

The algorithm review is the phase where the logical conclusion is given to the project. It includes all step by step processing of the project. The basic requirement of this phase is work plan ready and understood by all the actors involved. To discuss this phase, team has to be ready with technical and non-technical requirements of the project. In this proposed scheme, the data integrity, encryption and decryption is involved. Data integrity is the overall accuracy, completeness, and consistency of data. Data integrity also refers to the safety of data in regards to regulatory compliance. **It is maintained by a collection of processes, rules, and standards implemented during the design phase.** When the integrity of data is secure, the information stored in a database will remain complete, accurate, and reliable no matter how long it's stored or how often it's accessed. Data integrity also ensures that your data is safe from any outside forces. Whereas encryption uses blake2 algorithm to generate the key which induces data integrity for data securing and DCT is used for compression of the images.

V. TESTING

TC ID	Test Condition	Expected Outcome	Test Result
TC 1	When encoder or de-coder enters wrong password	Invalid password	Successful
TC 2	When encoder or de-coder enters the correct password	Login successful	Successful
TC 3	When decoder enters correct Key2	Image is decrypted	Successful
TC 4	When decoder enters wrong Key2	Image is not decrypted	Successful
TC 5	When an image is not of the order 8 x 8 is selected	Image is not encrypted	Unsuccessful

Figure 2: Test cases

Testing is a process of checking if the system is performing all the functions as per the requirements. The program to be tested is executed with a set of test cases and the output of the program for the test cases are evaluated to determine if the programming is performing as expected. The program to be tested is executed with a set of test cases and the output of the program for the test cases are evaluated to determine if the programming is performing as expected. Testing forms the first step in determining errors in a program. The success of testing in revelling errors in programs depends critically on the test case. Testing is mainly divided into two categories i.e., Black-box testing and white box testing. The success of testing in reveling errors in programs depends critically on the test case. Testing is mainly divided into two categories i.e., Black-box testing and white box testing

VI. RESULTS

(a) Original image *(b) Encrypted image*

Figure 3.1: Comparison between Original and Encrypted Image after Encryption.

Encryption is a process of translating original quantity into some other format, which provides data security. Figure 3.1 shows the results of the system during Encryption Operation. System is provided with original image (See in Figure 3.1 as input, then it generates an encrypted image (See in Figure 3.1 as a result. From the encryption results, it is observed as the encryption scheme can encrypt different size images, and all encrypted images are noise-like and meaningless. So the encrypted image gives no clue about the originality of the image so it is very difficult for the intruders to gain more knowledge and hence fails to perform different statistical attacks. It means the algorithm used can effectively encrypt images.

(b) Original image(b) Decrypted image

Figure 3.2: Comparison between Original and Encrypted Image after Encryption.

Decryption is a process of re-framing of original data from cipher format, which provides data visibility. Figure 3.2 shows and the comparison between original and decrypted image. System is provided with encrypted image (Bit stream) as input, then it generates decrypted image (See in Figure 3.2(b)) as a result, which looks similar to the original image with difference in size. From the decryption results, it is observed as the decryption scheme can decrypt different size encrypted images, and all decrypted images are similar to the corresponding original image and are meaningful. It means the algorithm can effectively decrypt images.

VII. CONCLUSION AND FUTURE WORK

The project is developed with an objective of balancing encryption and compression efficiency of the images. The aim is satisfied with the help of cryptographic techniques.] Future work is to extend the current encryption operations for other video/text compression standards, such as JPSEC standard and MPEG-4 and to support multiple end. Data integrity with more suitable algorithm can be involved for embedding key2 for security purposes.

REFERENCES

[1] Lingfeng Liu and SuoxiaMiao,"A New Image Encryption Algorithm based on Logistic Chaotic Map with Varying Parameter", Springer 2016..

[2] Ranjan Kumar H.S, FathimathSafeeriya S.P, SurendraShetty and Ganesh Aithal,"Image Encryption Based on Pixel Transposition and Lehmar Pseudo Random Number Generation", IEEE 2017.

[3] Hiba Abdel-Nabi and Ali Al-Haj, "Efficient Joint Encryption and Data Hiding Algorithm for Medical Images Security", IEEE 2017.

[4] LaiphrakpamDolendro Singh and KhumanthemManglem Singh, \Visually Mean ingful Multi-image Encryption Scheme" , Springer 2017..