Modern Cryptographic Approach For Image Encryption Scheme

M.D.Soumya[1], Ms.Vijetha[2]
[1]Dept of Computer Science and Engineering
[2]Associate Professor, Dept of Computer Science and Engineering
[1, 2] Srinivas Institute of Technology, Valachil, Mangaluru-575007

Abstract*- Images are the great source of information flowing across different info-generating platforms, to spread the facts in visualization than just raw facts. 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. But these operations have their own time constraints, so they should be carried out in a combined way to overcome this constraint and to have benefits of mutual picture compression and encryption. 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. Our picture encryption process composes an alternating new orthogonal transforms transformation, dc coefficients encryption, and ac coefficients encryption. To overcome the problem of continuously sending various secrete keys when the clear photo changes to the decoder, we embed the secrete key into the bit stream of some AC coefficients which is controlled by another key known as embedding key to get the position of embedded key position. Various tests are carried out to make sure that our system is strongly persistence to several crypt-analysis techniques.*

Keywords- Data insecurity; JPEG; Blake2; Compression, Encryption; Image-content-adaptive; secrete key;

I. INTRODUCTION

In past few years, massive amount of data has been getting created and transmitted through different social media platforms. However, these data need to be securely transmitted, safely stored and must be protected to being accessed by unauthorized users. One of the ways to secure the data from eavesdropping and unauthorized access is to encrypt the data or the channel and in some cases both.

Image form a major part of the data that is being transmitted in various social media platforms. Hence encrypting of images becomes more important. There have been many algorithms like Data Encryption Standard (DES), Advance Encryption Standard (AES) and many more for performing the encryption operations. But the majorproblem in using these algorithms is that the computational cost will be high since the size of the image data is often large and a small chunk of space gets removed, resulting in requesting further compression. Nowadays many algorithms are being proposed that uses different permutation only image encryption algorithms that result in increased speed and simpleoperations.

To avoid this “Modern Cryptographic Approach for Image Encryption Scheme” based on JPEG is used, which goals at enhancing the encryption power and also maintaining the efficiency ofcompression.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. This lacked in many compression-encryption techniques leading to failure of the system.

II. BACKGROUND

In [1], Zhou et al. designed a highly efficient image ETC system, where both lossless and lossy compression is considered. The proposed image encryption scheme operated in the prediction error domain is shown to be able to provide a reasonably high level of security. He also demonstrated that an arithmetic coding-based approach can be exploited to efficiently compress the encrypted images.

Peiya Li et al. [2], proposed a Joint image Compression and Encryption based on Alternating Transforms with controlled quality, a new joint image compression and encryption technique with controllable encryption parameters. This technique can achieve a sufficiently high level of security and preserve the good compression overall performance of JPEG, and it’s format compliant to JPEG format. Consequently, Shah et al. in [3] proposed a fast and robust encryption technique for gray scale medical images for real time applications. This technique first compresses the medical image in the discrete wavelet transform (DWT) domain before encrypting with an algorithm based on basic pixelpermutation and randomness. In the DWT domain, correlation and redundancy are reduced while random pixel permutation with encryption key provides confusion and diffusion.

Somaraj et al. [4], proposed a novel image Encryption approach the use of RGB pixel displacement for color images, a brand new technique for encrypting color images or 3D images using the concept of RGB displacement and scrambling is proposed. Bhatia et al. [5], proposed a unique image Enhancement technique based on Statistical analysis of DCT coefficients for JPEG Compressed photographs, the approach makes use of the statistical behavior of DCT coefficients extracted from the JPEG bit stream. The idea is inspired from the reality that the DC coefficient and the AC coefficients of a DCT block comply with unique distributions and subsequently desires to be analyzed separately.

III. DATA FLOW DIAGRAM

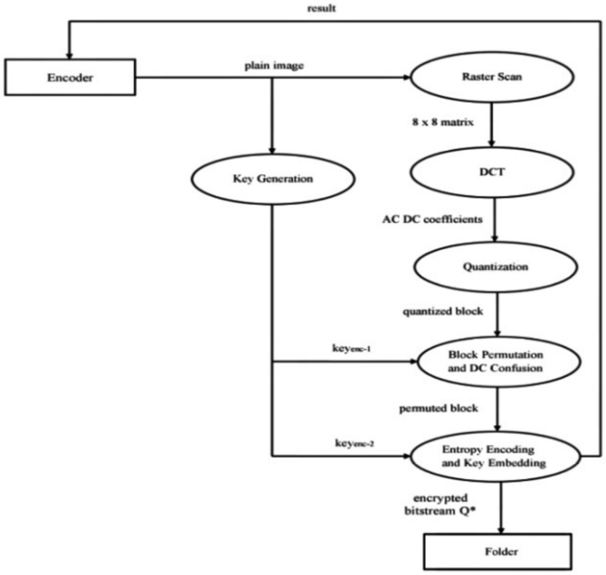

Figure 1: Data Flow Diagram of Secure Image System.

Fig 1 provides the data flow diagram for the system. Encoder provides the plain image as input, the compressed and encrypted image is stored as encrypted bitstream Q* in folder. The processes involved in Encoder are Raster scan, DCT, Quantization, Block Permutation and DC Confusion and Entropy Encoding and Key Embedding. Decoder provides the encrypted bitstream Q* from the folder as the input and receives the decrypted image from the system. The input is taken from Folder, the processes involved in Decoder are Entropy decoding Q* and extract key$_2$, Recover DC coefficients and inverse permutation, De-quantization, Inverse DCT to obtain the Plain Image from the Encrypted Compressed Image.

IV. IMPLEMENTATION

The implementation 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 implementation 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, it is explained in two steps, they are Encryption and Decryption.

A. Encryption Algorithm

```
Step 1: Upload Image I and enter Key$_2$.
Step 2: Obtain Key$_1$ from the plain image using
        blake 2 algorithm
Step 3: Feed Key$_1$and Key$_2$ to Blake2 to generate
        $K_{enc-1}$ and $K_{enc-2}$ keys.
Step 4: Perform raster scan on image to obtain 8 x 8
        blocks.
Step 5: for each 8 x 8 block do
Choose 63 bits from $K_{enc-1}$. Apply DCT twice
Transform 8 x 8 block and quantize it.
        end for
Step 6: Using $K_{enc-1}$ perform 8 x 8 blocks
Step 7: Confuse DC coefficients.
Step 8: Using $K_{enc-2}$ embed Key$_1$ into AC coefficients.
Step 9: Apply entropy encoding for all DC and AC
        coefficients to produce encrypted bit-stream
        Q*.
```

B. Decryption Algorithm

```
Step 1: Apply Blake2 on Key$_2$ to obtain $K_{enc-2}$.
Step 2: Apply entropy decoding on Q*to extract
Key$_1$ using Kenc-2.
Step 3: Generate by applying Blake2 on
Step 4: Recover confused DC coefficients.
Step 5: Perform de-permutation on 8 x 8 blocks using
        $K_{enc-1}$.
Step 6: for each 8 x 8 block do
          Perform dequantization.
Pick 63 bits from $K_{enc-1}$
Apply inverse DCT twice.
Inverse transform 8 x 8 blocks
end for
```

Step 7: Produce the decrypted image.

V. RESULT ANALYSIS

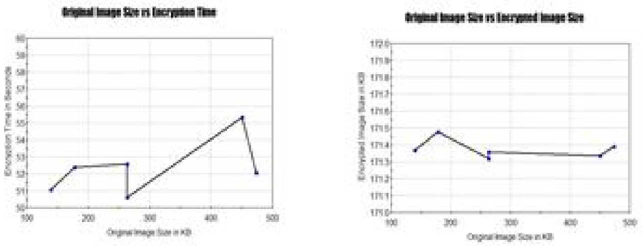

Figure 2: Graphs showing the Performance of the System during Encryption.

Figure 2 shows that for the different images of varying sizes, the time taken for its encryption varies apparently and also how the original image of various sizes varies with the different sizes of encrypted images obtained. Size of the original image largely influences on the quality of the encrypted image.

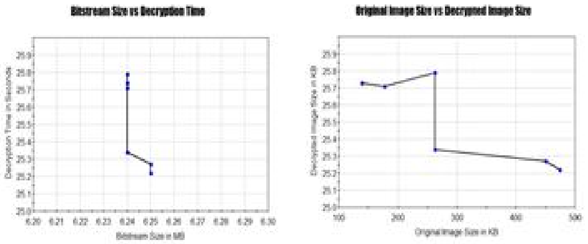

Figure 3: Graphs showing the Performance of the System during Decryption.

Figure 3 represents the performance of the system during decryption of the image. The size of the bitstream is compared with the decryption time. The decryption time varies for each bitstream depending on its size and also the original image size is compared with the decrypted image size which shows that the size of the decrypted images is always smaller than the original image due to the lossy JPEG compression.

VI. 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. The proposed scheme has good diffusion property and is compression friendly.

Future work is to extend our current encryption operations for other image/video compression standards, such as JPSEC standard and MPEG-4 and to support multiple end devices.

REFERENCES

[1] Jianta Zhou, Xianming Liu, Oscar C. Au and Yuan Yan Tang,“Designing an Efficient Emage Encryption-then-Compression System via Prediction Error Clustering and Random Permutation, IEEE2014.

[2] Peiya Li and Kwok-Tung Lo, “Joint Image Compression and Encryption Based on Alternating Transforms with Quality Control” , IEEE2015.

[3] Joshua ClebDagadu, Zian-Ping Li, Fadia Shah, Ndir Mustafa and Kamlesh Kumar, “DWT Based Encryption Scheme for Medical Images”, IEEE2016.

[4] ShrijaSomaraj and Mohammed Ali Hussain, “A Novel Image Encryption Technique Using RGB Pixel Displacement for Color Images”, IEEE2016.

[5] Jaspreeth Bhatia and Manish Okade, “A Novel Image Enhancement Technique Based on Statistical Analysis of DCT Coefficients for JPEG Compressed Images”, IEEE 2016