International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

GSVD Algorithm for Image Encryption

Smt. Suvarna Kabadi[1], Guide: Smt. Shruti Jalapur[2]

[1]PG Student at SIET College of Engineering and Technology Vijaypur, Karnataka, India
[2]Asst. Prof, CSE Dept of SIET College of Engineering and Technology Vijaypur, Karnataka, India

---

Abstract - *Cryptography is the technique to achieve the security my making the recognizable information into unrecognizable form. In this paper we used an algorithm called Generalized singular valued decomposition(GSVD) which supports only for RGB images in which a plain image is divided in two segments with a initial key, and key image or the reference image which is in exchanged form is used for encrypting and decrypting the original image. Mathematically speaking the read original image which is in matrix form, uses a initial key to generate two matrices and the GSVD algorithm with the key image matrix to get the matrix of cipher image. More security is achieved using this algorithm.*

Keywords: encryption, Decryption, SVD, GSVD.

1. INTRODUCTION

As we speak about Computer Networks, security is a must. To protect our important or confidential information security should be established during communication. There are many algorithms have been implemented to secure our data through communication and each algorithms will have their own processing time, which means the processing time of one algorithm may differ from another algorithm, some algorithms take more time and some algorithms takes less time, The algorithms which takes very less times that algorithm will be treated as the best algorithm. The processing time may vary depending upon the specifications of the machine as well as the versions of the software we used to develop the application. It is also very expensive to process large amount of the compressed data. One of the best methods to protect the data from others is to encrypt so that only the sender and receiver can access the information i.e only authorized persons can access the information. Here we call original image or the input image is called the plain image and output image is called the encrypted image or cipher image. Encryption and decryption which we commonly called as encoding and decoding of information. Using encryption algorithm the sender can send the information/original image in encoded form and only the authorized receiver can decode information. Here this algorithm is applied encryption and decryption of only color images, there are many algorithms which may be applied to text, audio and videos to protect their data. High security is the goal of this paper for colorful images which have been sent between recipients to keep them more secure from hackers.

1.1 Motivation

Today encryption is the technique is used to protect the important information from unauthorized access. To enhance the security of color images transmitted between the recipients. It is very expensive to encrypt the whole compressed bit stream. This algorithm works with the two keys the real number and the second is the key image which makes very difficult to break the cryptosystem by any person.

1.2 Problem Statement

In image communication system, the computational process of encryption and decryption with the compression and decompression of images which makes very difficult to handle large amount of information be processed and due to processing time this is very expensive.

1.3 Objective

Here the proposed algorithm is called Generalized Singular Valued Decomposition(GSVD) which supports only for RGB images in which a plain image is divided in two segments or parts with a initial key, and key image or the reference image which is in exchanged form, this key image is used for encrypting and decrypting the original image. Mathematically speaking the read original image which is in matrix form, uses a initial key to generate two matrices and the GSVD algorithm with the key image matrix to get the matrix of cipher image. This algorithm which is more secured compared to other image encryption algorithms as the images that has been transferred between the recipients are more secured.

2. PROPOSED METHODLOGY

The proposed algorithm is Generalised SVD algorithm using MATLAB R2018b latest version

2.1 Encryption Method

Read the Color Image, Split it into R,G and B Channel, Apply GSVD encryption algorithm on each channel of color image using encryption key, Combine three encrypted channel of the image i.e your encrypted image.

1. Start with image of any dimension rather than fixed as the algorithm is applied for any image and in any dimensions
2. Input an image of any size but here 200X200
3. Convert the image to Matrix I

4. Select an initial key K to generate the following matrices
   A1=K*I and A2=--K*I for all the RGB Channels
5. Choose an encrypting key image that can be converted to MatrixB
6. Compute the GSVD for each Matrix A1 and A2 with encrypting key Matrix B as the following

   [U1,V1,X1,C1,S1]=gsvd(I1,B) and
   [U2,V2,X2,C2,S2]=gsvd(I2,B)

7. Compute the following for all channnels

   A11=U1*C2*X1 and AA21=U2*C1*X

   Construct the encrypted image F such that
   F=[AA11+AA21]

8. Obtain the encrypted image F
9. End of Encryption Algorithm.

2.2 Decryption Method

Acquisition of encrypted image, Split it into R,G and B channel, Apply GSVD decryption algorithm on each channel of encrypted color image using decryption key(encryption key and decryption key should be same), Combine all three decrypted channel of color image i.e is your decrypted image.

1. Start
2. Download the encrypted image F
3. Obtain the Matrix of the Encrypted Image F
4. Split F into F1 And F2
5. Obtain the decrypted key matrix B which is similar to the encrypted key matrix
6. Compute the GSVD for each matrix F1 and F2 for all channels with the decrypting key matrix **B** as
   [U1,V1,X1,C1,S1]=GSVD(F1,B) and
   [U2,V2,X2,C2,S2]=GSVD(F2,B)
7. Compute the plain matrix I as the following
   A1=U1*C2*X1 for all channels
8. Out=Out/K to obtain the original image
9. End of Decryption Algorithm

3. EXPERIMENTAL RESULTS

Fig 1:Plain Img +Reference Img=Cipher Img

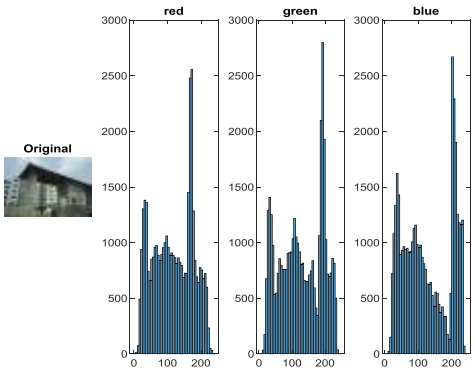

Fig 2: Before Encryption Histogram

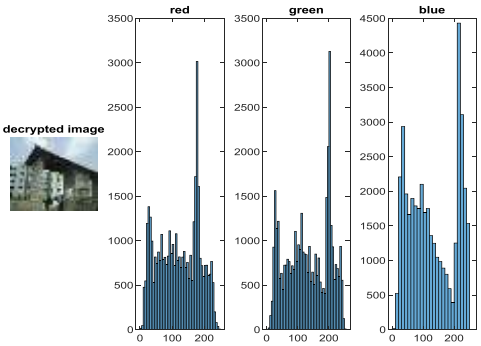

Fig 3: After Decryption Histogram

Table-1: Feature Extraction before and after Encryption and Decryption

File Type	JPG File
Size on Disk	3.68MB
Size after Encryption	235KB
Size after Decryption	65KB
Entropy B4 Encryption	7.7601
SD Before Encryption	0.6368
Elapsed Time for Encryption	2.818979
Elapsed Time for Decryption	0.915784
Entropy After Decryption	7.5151
SD for Decryption	0.6594

CONCLUSION

This algorithm is used for encryption and decryption of RGB images using MATLAB tool which involves compression and decompression of images, the time taken for encrypting and decrypting is less compared to other algorithms.

REFERENCES

[1] Selective Image Encryption using SVD and Arnold Transform Kshiramani Naik, Arup Kumar Pal, and Rohit Agarwal By The International Arab Journal of Information Technology, Vol. 15, No. 4, July 2018

[2] Key Logistic to Image Cryptography via General Singular Values Decomposition by Maheer Jalal Burjus Al-Bashkani , Prof. Dr. Adil Al Rammahi by JATIT on 15th July 2018

[3] A Singular value decomposition based approach for the compression of encrypted images HIyam Hatem, Raed Majeed Jumana Waleed by IJET 2018.

[4] Data Embedding into Image Encryption using the Symmetric Key for RDH in Cloud Storage by IJAER G. Preethi and N.P.Gopalan 2018

[5] Image Encryption Using Hybrid Chaotic Map Hikmat N. Abdullah, Hamsa A. Abdullah by 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT), Slemani – Iraq, ©2017 IEEE

[6] An Algorithm Based on GSVD for Image Encryption Mohammed Abdul Hameed Jassim AlKufi, Hayder Raheem Hashim Ameer Mohammed Hussein and Hind Rustum Mohammed, By MCA March 2017

[7] Image Encryption Based on Partitioning and Rearranged Pixels Position by Lebanese French niversity Dr. Jamila H. Al-A'meri, Salah T. Allawi, May M. Abbas April 2017

[8] Use the Singular Values Decomposition in the Text Encryption with Encryption Key Is Real Number Mohammed Abdul-Hameed Jassim Al-kufi University of Kufa, Najaf, Iraq by IJIRCCE, February 2016

[9] Image Encryption & Decryption with Symmetric Key Cryptography using MATLAB Jai Singh, Kanak Lata, and Javed Ashraf by International Journal of Current Engineering and Technology Feb 2015

[10] Analysis and Implementation of Selective Image Encryption Technique Using Matlab Upendra Bisht, Shubhashish Goswami by IOSR Journal of Computer Engineering (IOSR-JCE) in May-Jun. 2014.

[11] Image Encryption Based on Singular Value Decomposition, Nidhal K. El Abbadi, Adil Mohamad and Mohammed Abdul-Hameed by JCS July 2014