A SECURE AND HIGH CAPACITY DATAHIDING METHOD USING ARNOLD AND CHAOTIC SCRAMBLING ALGORITHM

Mrs.A.S.Malini[1],

Department of Computer Science Engineering,

P.S.R.Rengasamy College of Engineering For Women, Sivakasi, Tamil Nadu.

R.BHUVANESWARI[2], M.DEVIKA[3], K.MARIAMMAL[4],

Department of Computer Science Engineering,

P.S.R. College of Engineering for Women,

Sivakasi, Tamil Nadu.

---***---

Abstract:

In order to protect and secure the transmission of data over an open channel e.g. internet, an information security system must be in place. Cryptography and information hiding are the two branches of information security system. A high capacity data hiding method using lossless compression, advanced encrypted standard(AES), modified pixel value differencing(MPVD), and least significant bit(LSB) substation is presented. Arithmetic coding was applied on the secret key for the lossless compression, which provided 22%higher embedding capacity. The compressed secret message is subjected to AES encryption; This provide higher security in the cases of steganalysis attacks. After compression and encryption, the LSB substitution and MPVD are applied in this work. The proposed scheme is composed of Arnold Scrambling and Chaotic scrambling(SC-HAC). The security is considered by the proposed scheme which combines Arnold scrambling and Logistic scrambling to improve the encryption effect. MATLAB tool used to verify our proposed algorithm.

KEYWORDS: Digital Images, Steganography, Arnold transform, Data Hiding, Image Encryption.

1. Introduction

Due to the fast development of network related technologies, visual data communication through the internet become prevalent. Consequently, to prevent the data security problem, example. illegal interception and duplication, through the internet, information forensics is essential. In this paper, we present a data hiding method for absolute moment block truncation coding compressed images. In the past few years, many image based data hiding technique have been proposed to protect the hidden n data and guarantee secrecy of the visual data. On the basics of their application, most of them classified into two categories(1) steganography / encryption, where steganography is achieved by scattering the hidden data in each pixel, and the secret message has no connection to the stego image. The purpose of steganography is to protect the secret data only, not the cover image. Therefore, recovering the host image is not necessary for this type of application.

1.1Image compression:

Most transmitted images are compressed first to reduce the file size and increase the network transmission efficiency. The commonly used compression methods typically are divided into four groups: lossy compression, lossless compression predictive compression and transform compression. In lossy compression method, gradual changes of color are maintained and sudden changes of color are removed. In lossless compression methods, the quality of image or video is not degraded. Predictive compression involves high correlation between local space and time limit in image signals.

2. Related work:

A secure multiple watermarking method based on discrete wavelet transform(DWT),discrete cosine transform(DCT)and singular value decomposition(SVD). For identity authentication purpose, the proposed method uses medical image as the image water mark, and personnel and medical record of patient as the text water mark. In the embedding process, the cover medical image is decomposed up to second level of DWT coefficient.

The robust life cycle water marking approach using transform domain technique for telehealth application. The patient identity is embedding into the host medical image for the purpose of authentication, annotation and identification. Experimental results clearly indicated the highly robust and sufficient secure for various form of attacks without any significant distortion between watermarked and cover image.

Dual image reversible data hiding scheme, divide a secret message into sub-stream of size n bit, where n-1 bits embedded using pixel value differencing(PVD)and one bit embedded using Difference Expansion(DE). With extract the secret message successfully and recover original cover image from dual stego image without any distortion.

A secure medical image watermarking technique applying spectrum concept in wavelet transform domain is proposed. Discrete wavelet transform(DWT) decomposes the cover medical image into four frequencies sub-bands using Mexican hat as mother wavelet. The impersability of the water marked image, strength of generated PN sequence pair is adjusted according to specify document to watermark ratio.

A novel prediction-based reversible steganographic scheme based on image in painting. Reference pixel are chosen adaptively according to the distributed characteristics of the image content. The proposed scheme provides the greater embedding rate and better visual quality compared with recently reported methods.

3. Existing System:

3.1 Compression through arithmetic coding:

The compression is achieved through arithmetic coding. In arithmetic coding, fewer bits are used for frequently used character and in frequently used characters are stored with more number of bits, thus, resulting in fewer bits required for total encoding. After compression, output of this step would be a bit stream of compressed secret images. Extra '0' bits are added at the end, if required, to make the sequence divisible by 8. This bit stream is used as input for AES based encryption.

3.2Encryption using AES:

Input: 128-bit data**,**128-bit key,

output: Cipher text

Steps involved:

a. Sub Bytes()

b. Shift Rows()

c. Mix Columns()

d. Add Roundkey()

Steps c is not required in the final round.

3.3. Decryption using AES:

For each round, with the state and key as input (expect for last round), following steps are repeated:

Step1: Inverse_Sub Bytes()

Step2:Inverse _Shift Rows()

Step3:Inverse_Mix Columns()

Step4:Inverse_Add Roundkey()

Step 3 is not performed for last round. All the encryption steps should be performed in reverse to achieve decryption.

4. Proposed system:

The proposed scheme is composed of hash function, Arnold scrambling and chaotic scrambling (SC-HAC). For the adaptiveness problem, our scheme uses semi tensor compressive sensing to encrypt multiple signal with different dimensions. The chaotic sequence is applied to generate the semi tensor measurement matrix. On the one hand , we only transmit a few chaotic parameters, which reduce the number of data storage and transmission. On the other hand, the size of the measurement matrix is small, and the computation overhead can be reduced. The security is considered by the proposed scheme which combines Arnold scrambling and Logistic scrambling to improve the encryption effect.

4.1Key Generation:

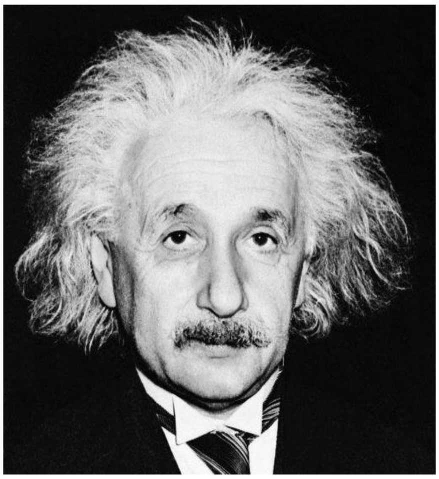
For the SHA-256 Hash function , the length of the input is arbitrary, and the length of the output is 256 bits in this paper, a plain images is used as input, and the output of the hash function is treated as the key.

4.2. Encryption and compression:

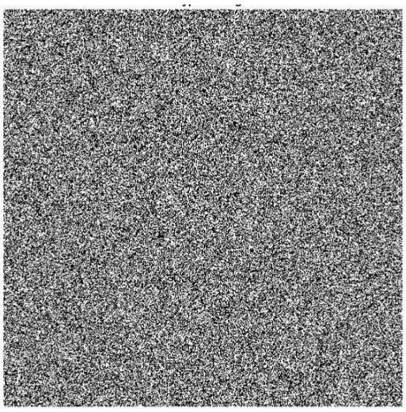
The model of semi tensor product compressive sensing (STP-CS), which shows the process of semi tensor compressive sensing. The initial sampling position is arbitrary. For convenience, it is set as own. In order to reduce the correlation of the Logistic sequence, the sampling interval is set as 4 empirically. So the sequence s can be obtained.

5. Result Analysis:

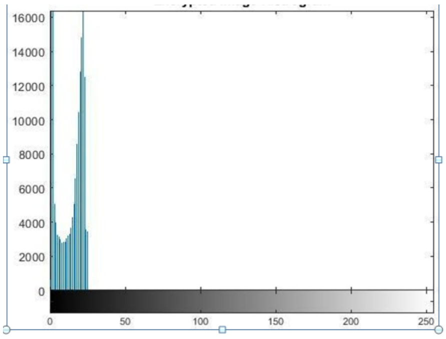
5.1Encryption process:



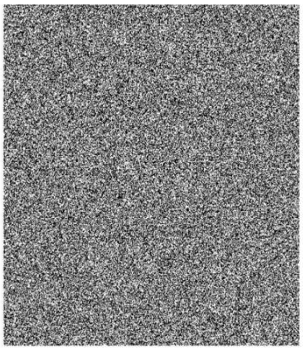
5.2 Encrypted Image:



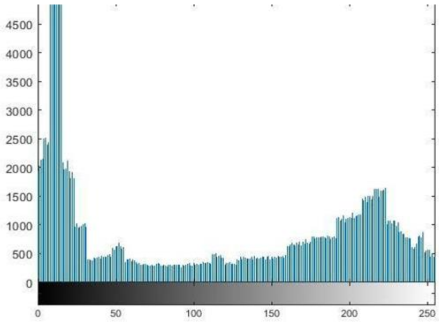
5.3 Input encrypted image histogram:



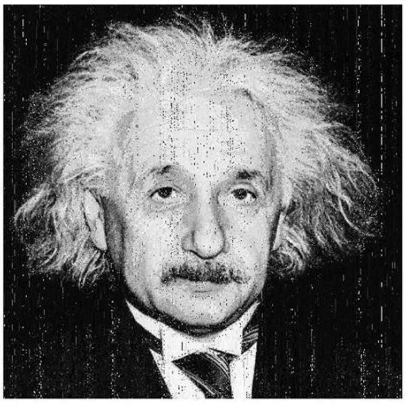
5.4 Decryption process:



5.5 Output decrypted histogram:



5.6 Decrypted image:



6. Conclusion:

In this project, a secure and high capacity image steganography method is proposed in which the arithmetic coding is used for high embedding capacity; AES for additional security of hidden contents; MPVD,LSB and pixel optimization for enhanced capacity and improved visual capacity. In MPVD, lower embedding rates was opted at higher ranges. An enhanced capacity of 3% more than earlier methods has been achieved using MPVD.MPVD and Arithmetic coding together resulted in 25% in higher embedding. Also, the proposed methods is secure against RS steganalysis. Thus, proposed scheme promises significant advancement over existing methods.

7. References:

[1]K.Shukla,Kankash singh, Balvindar singh,„,,"A secure and high capacity data hiding method using compression",2018.

[2]M.Hussain,A.W.A.Waheb,N.Javed and K,H.Jung,„,,"Recursive information hiding scheme through LSB,PVD shift and MPE"IETE Tech. Rev., vol. 35, no. 1, pp. 53–63, 2018.

[3]P.Pal,P.Chowdhuri,and B.Jana,„,,Reversible watermarking scheme using PVD-DE,""inProc.int.conf.Comput.Intell.,Commun.Bus.Anal.,2017,pp.511-524.

[4]A.K.Singh,B.Kumar, G.Singh and A.Mohan, Medical Image Watermarking: Techniques and Applications.New York,NY,USA:Springer,2017.

[5]C.Kumar, A.K.Singh,and P.Kumar, „,,Improved wavelet-based image watermarking through SPIHT,"' in Multimedia Tools and Applications. New York,NY,USA:Springer,2018,pp.1-14.